Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/018182

International filing date: 07 December 2004 (07.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-182180
Filing date: 21 June 2004 (21.06.2004)

Date of receipt at the International Bureau: 03 February 2005 (03.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/JP2004/018182

日本国特許庁
JAPAN PATENT OFFICE

09.12.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

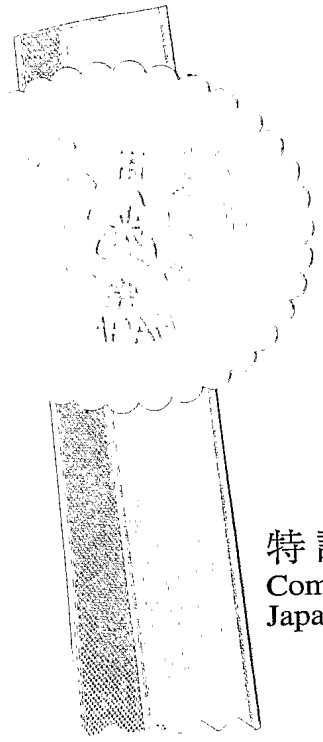
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　６月２１日

出願番号
Application Number: 特願２００４－１８２１８０

[ST. 10/C]: ［ＪＰ２００４－１８２１８０］

出願人
Applicant(s): 石井　美恵子



２００５年　１月２１日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３１２３３０７

【書類名】　特許願
【整理番号】　TUP0401
【特記事項】　特許法第４４条第１項の規定による特許出願
【提出日】　平成16年 6月21日
【あて先】　特許庁長官　殿
【原出願の表示】
　【出願番号】　特願2003-408568
　【出願日】　平成15年12月 8日
【国際特許分類】　G06F 17/60
【発明者】
　【住所又は居所】　京都府京都市下京区松原通東洞院東入本燈篭町１１番地
デリート烏丸東５０４号室
　【氏名】　塚本　豊
【特許出願人】
　【住所又は居所】　岡山県倉敷市羽島２２１番地の４
　【氏名又は名称】　石井　美恵子
【代理人】
　【識別番号】　100104433
　【弁理士】
　【氏名又は名称】　宮園　博一
【手数料の表示】
　【予納台帳番号】　073613
　【納付金額】　16,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
個人ユーザに関する固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を監視するためのプライバシー保護方法であって、
購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガードステップと、
前記個人ユーザが顧客またはユーザとして所定の業者に自己のメールアドレスを通知するときに、当該業社用としての新たな通知用メールアドレスであって当該業社を特定する情報を割出すことができる通知用メールアドレスを生成して当該業社に通知するための処理を行うメールアドレス通知処理ステップと、
前記メールアドレス通知処理ステップにより前記通知用メールアドレスを通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成ステップと、
識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成ステップにより生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信ステップと、
送信元から送信された電子メールを指定されたメールアドレスに従って送信先に送信するための電子メール送信ステップと、
該電子メール送信ステップにより送信される電子メールの送信先のメールアドレスが、前記メールアドレス通知処理ステップにより通知した前記通知用メールアドレスである場合に、当該通知用メールアドレスに対応する前記通知業社を特定する情報を割出し、該割出された通知業社を特定する情報と当該電子メールの送信元の情報とが一致するか否か監視する監視ステップとを含むことを特徴とする、プライバシー保護方法。
【請求項２】
個人ユーザに関する固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を監視するためのプライバシー保護システムであって、
前記個人ユーザが顧客またはユーザとして所定の業者に自己のメールアドレスを通知するときに、当該業社用としての新たな通知用メールアドレスであって当該業社を特定する情報を割出すことができる通知用メールアドレスを生成して当該業社に通知するための処理を行うメールアドレス通知処理手段と、
前記メールアドレス通知処理手段により前記通知用メールアドレスを通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成手段と、
識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成手段により生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信手段と、
送信元から送信された電子メールの送信先のメールアドレスが、前記メールアドレス通知処理手段により通知した前記通知用メールアドレスである場合に、当該通知用メールアドレスに対応する前記通知業社を特定する情報を割出し、該割出された通知業社を特定する情報と当該電子メールの送信元の情報とが一致するか否か監視する監視手段とを含むことを特徴とする、プライバシー保護システム。
【請求項３】
前記メールアドレス通知処理手段は、メールアドレスを通知する通知業社を特定するための通知業社特定情報を含むデータを暗号化して前記通知用メールアドレスを生成する暗号化生成手段を含み、
前記監視手段は、
送信元から送信された電子メールの通知用メールアドレスを復号する復号手段と、

該復号手段により復号されたデータ中に含まれている前記通知業社特定情報と当該電子メールの送信元の情報とが一致するか否かを判定する判定手段とを含むことを特徴する、請求項２に記載のプライバシー保護システム。

【請求項４】

前記通知業者は、商品を販売する販売店であり、

前記メールアドレス通知処理手段は、前記販売店においてポイントカードの発行に伴うユーザ登録の際に当該販売店に対応する通知用メールアドレスを生成して通知する処理を行い、

前記発信手段は、前記販売店において購入する商品に付されている無線識別子発信装置から発信される固有の識別子を利用して割出される当該商品の販売価格に従って自動決済を行う際に、前記無線識別子発信装置の前記固有の識別子を読取るための識別子送信要求があった場合に、前記販売店に対応する前記通知業者用識別子を発信することを特徴とする、請求項２または請求項３に記載のプライバシー保護システム。

【請求項５】

個人ユーザに関する固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を監視するためのプライバシー保護用識別子発信装置であって、

前記個人ユーザが顧客またはユーザとなった所定の業者のために新たな通知用メールアドレスを生成して当該業社に通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成手段と、

識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成手段により生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信手段とを含むことを特徴とする、プライバシー保護用識別子発信装置。

【書類名】明細書
【発明の名称】プライバシー保護方法、プライバシー保護システムおよびプライバシー保護用識別子発信装置
【技術分野】
【０００１】
本発明は、たとえばＩＣタグ（ＲＦＩＤタグ）等から発信されたＲＦＩＤ（Radio Frequency Identification）等の固有の識別子が読取られて該固有の識別子に基づくプライバシーの侵害を監視するための、プライバシー保護方法、プライバシー保護システムおよびプライバシー保護用識別子発信装置に関する。
【背景技術】
【０００２】
メーカーで製造された商品が卸売業者等の中間流通業者に出荷された後小売店に入荷されるその商品の流通段階で当該商品を管理するために、その商品にＲＦＩＤタグを付するという提案がなされている（たとえば、特許文献１）。
【０００３】
この背景技術では、メーカーからの出荷時、中間流通業者への入荷時、小売店での入荷時、消費者の購入時等の流通段階における要所要所において、商品に付されているＲＦＩＤタグに記憶されているＲＦＩＤをタグリーダが読取り、当該ＲＦＩＤが正規に登録されている適正なものであるか否かをチェックし、商品が正しく流通しているか否かを監視する。
【０００４】
また、例えば、デパート等の小売店で購入したＲＦＩＤタグ付きの商品を購入者が袋に詰め、その袋を持って小売店の通過ゲートを通過する際に、その通過ゲートに設けられているタグリーダと購入商品に付されているＲＦＩＤタグとが交信し、ＲＦＩＤタグから送信されてきたＲＦＩＤに基づいて各商品の価格を自動的に割出してその合計を算出し、購入者が所持している決済機能付の携帯電話やＩＣカード等と交信して自動決済を行なう方法が提案されている（たとえば、特許文献２参照）。
【特許文献１】特開２０００－１６９２２９
【特許文献２】特開２０００－１９６５５５
【発明の開示】
【発明が解決しようとする課題】
【０００５】
このように、種々の商品に付されたＲＦＩＤタグは、タグリーダからのＲＦＩＤ送信要求に応じて記憶しているＲＦＩＤを自動的に発信するために、商品が例えば衣服や眼鏡や指輪やイヤリングや腕時計等のように、常時身に付けて携帯される物の場合には、当該商品が個人ユーザに購入された後においても、タグリーダからのＲＦＩＤ送信要求に応じて当該個人ユーザが身に付けている商品のＲＦＩＤタグからＲＦＩＤが発信されることとなる。その結果、当該個人ユーザのプライバシーが侵害される虞が生ずる。
【０００６】
たとえば、前述の自動決済を行うの際に、タグリーダからのＲＦＩＤ送信要求に応じて、購入者が身に付けている購入済み商品に付されているＲＦＩＤタグからもＲＦＩＤが発信されることとなる。
【０００７】
その結果、たとえば或る個人ユーザであるアリスが、Ａデパートの婦人服売り場のマタニティーコーナーで岩田帯（腹帯）を購入してその商品に付されているＲＦＩＤタグをタグリーダに読み取らせて自動決済を行なった後、食器売り場で夫婦茶碗を購入してその商品に付されているＲＦＩＤタグをタグリーダに読取らせて自動決済を行なった場合には、その個人ユーザアリスが常時携帯している購入済み商品に付されているＲＦＩＤタグも同時に読み取られることとなる。そのＲＦＩＤタグのＲＦＩＤが例えば、１２３４５６であった場合には、１２３４５６のＲＦＩＤを発信するＲＦＩＤタグの商品を常時携帯してい

る同一人物が岩田帯(腹帯)を購入するとともに夫婦茶碗も購入したことがわかってしまい、その個人ユーザは、おそらく、結婚前に妊娠していることが推測できてしまう。

【０００８】

しかも、ＲＦＩＤタグのＲＦＩＤを利用した自動決済の際に、そのＡデパートのポイントカードによるポイント加算処理も合わせて行なった場合には、そのポイントカードの新規発行時にユーザ登録している個人名（アリス）や住所やＥメールアドレス等の個人特定情報がつきとめられ、前述したＲＦＩＤ１２３４５６を発するＲＦＩＤタグを常時携帯している人物はアリスであることが見破られてしまう。

【０００９】

さらに、個人名、住所、Ｅメールアドレス等の個人特定情報と当該個人から発せられる固有の識別情報（ＲＦＩＤ等）とが一旦リンクされ、そのリンクされた個人特定情報に前述の結婚前に妊娠している旨の個人情報が加えられたものが漏洩されて闇ルートを介して流通した場合には、次のようなプライバシーに関する深刻な問題が生じる。

【００１０】

たとえば、個人（アリス）が前述の漏洩された固有の識別情報を発信する発信装置（ＲＦＩＤタグ等）を身に付けて外出し、たとえば書店、ＣＤショップ、百貨店等を渡り歩き、その先々で身に付けている識別子発信装置（ＲＦＩＤタグ等）が読取られてその固有の識別情報（ＲＦＩＤ等）に基づいて前述の漏洩した個人情報が検索され、後に、たとえば、妊娠中のセックスに関する書籍の電子メール、妊娠中に適した音楽ＣＤの電子メール、赤ちゃんのおもちゃの電子メール等の大量の迷惑メール（スパム）やダイレクトメールが届くようになる。

【００１１】

そこで、このような問題を防止するべく、商品購入時にその商品に付されているＲＦＩＤタグのＲＦＩＤ発信機能を作動不能状態に切換えるようにし、購入済商品を消費者が身につけたとしても、その商品からＲＦＩＤが発信されることがないように構成することが考えられる。

【００１２】

しかし、このように構成した場合には、購入済商品に付されたＲＦＩＤタグから発せられるＲＦＩＤを利用して種々のサービスを享受することができないという不都合が生ずる。購入済み商品のＲＦＩＤタグのＲＦＩＤを利用したサービスとしては、例えば、商品のＲＦＩＤタグから発せられるＲＦＩＤ毎に分類して当該商品の詳細な情報を登録しているサーバに消費者がＲＦＩＤのコードを送信してアクセスし、当該ＲＦＩＤに対応する商品情報を検索して入手することや、商品が例えばパーソナルコンピュータ等であった場合にソフトウェアのバージョンアップ情報の提供等が考えられる。

【００１３】

このようなＲＦＩＤを利用したサービスを消費者が享受できるようにするためには、例えば、携帯電話等を利用して消費者自身が購入済商品に付されているＲＦＩＤタグをたとえば発信停止状態等にしてＲＦＩＤガード状態にし、かつ、ＲＦＩＤ発信可能状態等のＲＦＩＤガード解除状態に切換えることができるように構成することが考えられる。しかし、消費者の操作等によってＲＦＩＤタグが発信状態（ＲＦＩＤガード解除状態）あるいは発信停止状態（ＲＦＩＤガード状態）に切換え可能にした場合には、発信停止状態（ＲＦＩＤガード状態）にすべき時に消費者（個人ユーザ）が発信停止状態（ＲＦＩＤガード状態）にすることを忘れて怠ってしまう虞が生ずる。その場合には、前述したプライバシーの侵害問題が発生することとなる。

【００１４】

また、購入済商品に付されているＲＦＩＤタグを発信停止状態や発信可能状態に切換えるための操作機能を有する新たな携帯電話等の操作装置を個人ユーザが購入しない限り、そのようなモードの切換えができないのであり、モード切換え機能を有する操作装置を有しない個人ユーザの場合には、購入済商品のＲＦＩＤタグが常にＲＦＩＤ発信状態つまり、常に前述したプライバシーの侵害問題が発生する状態となるという虞がある。

【００１５】
さらに、今後ＲＦＩＤタグが普及してタグリーダがいたるところに設置された場合には、いたるところで前述のプライバシー問題が頻発することになるとともに、同一コードのＲＦＩＤを追跡することにより個人ユーザの移動追跡が行なわれてしまうという虞も生じる。

【００１６】
本発明は、係る実情に鑑み考え出されたものであり、その目的は、固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を監視することである。

【課題を解決するための手段】

【００１７】
請求項１に記載の本発明は、個人ユーザに関する固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を監視するためのプライバシー保護方法であって、

購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガードステップと、

前記個人ユーザが顧客またはユーザとして所定の業者に自己のメールアドレスを通知するときに、当該業社用としての新たな通知用メールアドレスであって当該業社を特定する情報を割出すことができる通知用メールアドレスを生成して当該業社に通知するための処理を行うメールアドレス通知処理ステップと、

前記メールアドレス通知処理ステップにより前記通知用メールアドレスを通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成ステップと、

識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成ステップにより生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信ステップと、

送信元から送信された電子メールを指定されたメールアドレスに従って送信先に送信するための電子メール送信ステップと、

該電子メール送信ステップにより送信される電子メールの送信先のメールアドレスが、前記メールアドレス通知処理ステップにより通知した前記通知用メールアドレスである場合に、当該通知用メールアドレスに対応する前記通知業社を特定する情報を割出し、該割出された通知業社を特定する情報と当該電子メールの送信元の情報とが一致するか否か監視する監視ステップとを含むことを特徴とする。

【００１８】
請求項２に記載の本発明は、個人ユーザに関する固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を監視するためのプライバシー保護システムであって、

前記個人ユーザが顧客またはユーザとして所定の業者に自己のメールアドレスを通知するときに、当該業社用としての新たな通知用メールアドレスであって当該業社を特定する情報を割出すことができる通知用メールアドレスを生成して当該業社に通知するための処理を行うメールアドレス通知処理手段と、

前記メールアドレス通知処理手段により前記通知用メールアドレスを通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成手段と、

識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成手段により生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信手段と、

送信元から送信された電子メールの送信先のメールアドレスが、前記メールアドレス通

知処理手段により通知した前記通知用メールアドレスである場合に、当該通知用メールアドレスに対応する前記通知業社を特定する情報を割出し、該割出された通知業社を特定する情報と当該電子メールの送信元の情報とが一致するか否か監視する監視手段とを含むことを特徴とする。

【００１９】

請求項３に記載の本発明は、請求項２に記載の発明の構成に加えて、前記メールアドレス通知処理手段は、メールアドレスを通知する通知業社を特定するための通知業社特定情報を含むデータを暗号化して前記通知用メールアドレスを生成する暗号化生成手段を含み、

前記監視手段は、

送信元から送信された電子メールの通知用メールアドレスを復号する復号手段と、

該復号手段により復号されたデータ中に含まれている前記通知業社特定情報と当該電子メールの送信元の情報とが一致するか否かを判定する判定手段とを含むことを特徴する。

【００２０】

請求項４に記載の本発明は、請求項２または請求項３に記載の発明の構成に加えて、前記通知業者は、商品を販売する販売店であり、

前記メールアドレス通知処理手段は、前記販売店においてポイントカードの発行に伴うユーザ登録の際に当該販売店に対応する通知用メールアドレスを生成して通知する処理を行い、

前記発信手段は、前記販売店において購入する商品に付されている無線識別子発信装置から発信される固有の識別子を利用して割出される当該商品の販売価格に従って自動決済を行う際に、前記無線識別子発信装置の前記固有の識別子を読取るための識別子送信要求があった場合に、前記販売店に対応する前記通知業者用識別子を発信することを特徴とする。

【００２１】

請求項５に記載の本発明は、個人ユーザに関する固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を監視するためのプライバシー保護用識別子発信装置であって、

前記個人ユーザが顧客またはユーザとなった所定の業者のために新たな通知用メールアドレスを生成して当該業社に通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成手段と、

識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成手段により生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信手段とを含むことを特徴とする。

【発明の効果】

【００２２】

請求項１に記載の本発明によれば、個人ユーザが所定の業社に自己のメールアドレスを通知するときに当該業社用としての新たな通知用メールアドレスであって当該業社を特定する情報を割出すことができる通知用メールアドレスを生成して当該業社に通知する。そして、識別子の送信要求があった場合には、個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を当該個人ユーザの意思に従って他人が読取れない識別子ガード状態した上で、通知用メールアドレスを通知した相手である通知業社に対し当該通知業社に対応した通知業社用識別子を生成して毎回同じ通知業社用識別子を発信する。この状態で、仮に通知業社に通知した通知用メールアドレスと通知業社に発信した通知業社用識別子とがリンクされてその個人情報が漏洩されたとしても、自己の個人情報がどこの通知業社から漏洩されたかを次のようにして割出すことができる。

【００２３】

識別子の発信要求に応じて、前述の通知業社以外の者に対し識別子を発信する場合であっても、前述の通知業社用識別子を発信する旨の個人ユーザの操作があった場合には、前述の通知業社用識別子が発信される。その通知業社用識別子を受信した者がその通知業社用識別子に基づいて漏洩された個人情報を検索して該当する個人情報を割出し、その個人情報中に含まれている前述の通知用メールアドレスに基づいて電子メールを個人ユーザに送信した場合には、当該通知用メールアドレスが前述の通知業社用として新たに生成された当該通知業社用のメールアドレスであるために、その通知用メールアドレスからそれを通知した相手である通知業社を特定する情報を割出すことができる。そして、その割出した通知業社を特定する情報と電子メールを送信してきた送信元の情報とが一致するか否かを監視し、一致しない場合には、当該電子メールの送信元が前述の通知業社から漏洩された個人情報に基づいて電子メールを送信してきた可能性が高いことが明らかとなる。

【００２４】

このような電子メールの送信元とその電子メールの通知用メールアドレスとの整合性チェックによる監視により、どこの通知業社が個人情報を漏洩させた可能性が高いかが判明されるとともに、電子メールを送信してきた送信元が漏洩された個人情報を入手して電子メールを送信してきた可能性が高いことが判明できる。これにより、漏洩された個人情報を利用しての電子メールの送信を抑止する効果が期待できる。

【００２５】

請求項２に記載の本発明によれば、個人ユーザが所定の業社に自己のメールアドレスを通知するときに当該業社用としての新たな通知用メールアドレスであって当該業社を特定する情報を割出すことができる通知用メールアドレスを生成して当該業社に通知する。そして、識別子の送信要求があった場合には、通知用メールアドレスを通知した相手である通知業社に対し当該通知業社に対応した通知業社用識別子を生成して毎回同じ通知業社用識別子を発信する。この状態で、仮に、通知業社に通知した通知用メールアドレスと通知業社に発信した通知業社用識別子とがリンクされてその個人情報が漏洩されたとしても、自己の個人情報がどこの通知業社から漏洩されたかを次のようにして割出すことができる。

【００２６】

識別子の発信要求に応じて、前述の通知業社以外の者に対し識別子を発信する場合であっても、前述の通知業社用識別子を発信する旨の個人ユーザの操作があった場合には、前述の通知業社用識別子が発信される。その通知業社用識別子を受信した者がその通知業社用識別子に基づいて漏洩された個人情報を検索して該当する個人情報を割出し、その個人情報中に含まれている前述の通知用メールアドレスに基づいて電子メールを個人ユーザに送信した場合には、当該通知用メールアドレスが前述の通知業社用として新たに生成された当該通知業社用のメールアドレスであるために、その通知用メールアドレスからそれを通知した相手である通知業社を特定する情報を割出すことができる。そして、その割出した通知業社を特定する情報と電子メールを送信してきた送信元の情報とが一致するか否かを監視し、一致しない場合には、当該電子メールの送信元が前述の通知業社から漏洩された個人情報に基づいて電子メールを送信してきた可能性が高いことが明らかとなる。

【００２７】

このような電子メールの送信元とその電子メールの通知用メールアドレスとの整合性チェックによる監視により、どこの通知業社が個人情報を漏洩させた可能性が高いかが判明されるとともに、電子メールを送信してきた送信元が漏洩された個人情報を入手して電子メールを送信してきた可能性が高いことが判明できる。これにより、漏洩された個人情報を利用しての電子メールの送信を抑止する効果が期待できる。

【００２８】

請求項３に記載の本発明によれば、請求項２に記載の本発明の効果に加えて、メールアドレスを通知する通知業社を特定するための通知業社特定情報を含むデータを暗号化することにより前述の通知用メールアドレスが生成され、電子メールの送信元と通知用メールアドレスとの整合性チェックによる監視においては、送信元から送信された電子メールの

通知用メールアドレスを復号し、その復号されたデータ中に含まれている通知業社特定情報と当該電子メールの送信元の情報とが一致するかを判定して整合性のチェックを行う。その結果、送信されてきた電子メールの通知用メールアドレス自体に整合性チェックのための通知業社を特定する通知業社特定情報が含まれており、復号することによりその通知業社特定情報を容易に入手することができ、整合性チェックが行い易くなる。

【００２９】

請求項４に記載の本発明によれば、ポイントカードの発行に伴うユーザ登録を行った販売点において購入する商品に付されている無線識別子発信装置から発信される固有の識別子を利用して割出される当該商品の販売価格に従って自動決済を行う際に、無線識別子発信装置の固有の識別子を読取るための識別子送信要求があった場合には、当該販売店に対応する通知業社用識別子が発信されるために、自動決済を行うことができながらも、当該販売店から漏洩された個人情報に基づいた電子メールが送信されてきた場合に、前述の整合性チェックによる監視が可能となる。

【００３０】

請求項５に記載の本発明によれば、識別子の発信要求に応じて、通知業社以外の者に対し識別子を発信する場合であっても、通知業社用識別子を発信する旨の個人ユーザの操作があった場合には、通知業社用識別子が発信される。その通知業社用識別子を受信した者がその通知業社用識別子に基づいて漏洩された個人情報を検索して該当する個人情報を割出し、その個人情報中に含まれている前述の通知用メールアドレスに基づいて電子メールを個人ユーザに送信した場合には、当該通知用メールアドレスが前述の通知業社用として新たに生成された当該通知業社用のメールアドレスであるために、その通知用メールアドレスからそれを通知した相手である通知業社を特定する情報を割出すことができる。そして、その割出した通知業社を特定する情報と電子メールを送信してきた送信元の情報とが一致するか否かを監視し、一致しない場合には、当該電子メールの送信元が前述の通知業社から漏洩された個人情報に基づいて電子メールを送信してきた可能性が高いことが明らかとなる。

【００３１】

このような電子メールの送信元とその電子メールの通知用メールアドレスとの整合性チェックによる監視により、どこの通知業社が個人情報を漏洩させた可能性が高いかが判明されるとともに、電子メールを送信してきた送信元が漏洩された個人情報を入手して電子メールを送信してきた可能性が高いことが判明できる。これにより、漏洩された個人情報を利用しての電子メールの送信を抑止する効果が期待できる。

【発明を実施するための最良の形態】

【００３２】

次に、本発明の実施の形態を図面に基づいて詳細に説明する。図１は、ブロードバンドを利用したネットワークシステム全体の概略を示す構成図である。広域・大容量中継網４３を通じて、クレジットカード発行会社群４、加盟店契約会社群５、受信局４２、加盟店群６、サプライヤ群Ｓ、ＮＭ群（ニューミドルマン群）４８、電子行政群４９、ＸＭＬストア５０、コンテンツプロバイダ群５１、信号５２、携帯電話網５４に接続されたゲートウェイ５３、インターネットＩ、ユーザ宅４７、認証局群４６、コンビニエンスストア群２、会社群４５、データセンタ４４、ライフ支援センタ８、放送局４１、金融機関群７等が、情報の送受信ができるように構成されている。なお、図中４０は衛星（サテライト）であり、放送局４１からの放送電波を中継して受信局４２に電波を送るためのものである。

【００３３】

クレジットカード発行会社群４とは、たとえばＳＥＴ（Secure Electronic Transaction）により決済を行なう場合のイシュアとしての機能を発揮するカード発行会社である。加盟店契約会社群５は、電子モール等を構成する加盟店群６が契約している金融機関等からなる会社であり、ＳＥＴにおけるアクアイアラとして機能する機関である。サプライヤ群Ｓとは、商品メーカー等であり、商品や情報を提供する機関のことである。ＮＭ群４８

とは、サプライヤ群Ｓと消費者（自然人または法人）との仲立ちを行ない、たとえば消費者のショッピング等の消費行動の支援を行なうサービス業者のことである。従来の問屋や商社等の中間業者が、サプライヤ群の販売支援を行なうのに対し、このＮＭ群４８は、消費者の購入支援（消費行動支援）を行なう点で相違する。ＮＭ群４８の具体例としては、消費者の嗜好情報や購買履歴情報やＷｅｂサイトへのアクセス履歴情報をデータベースとして蓄積し、その蓄積されている消費者のプロフィール情報（個人情報）に基づいてその消費者にマッチする商品情報等を推薦して、消費者の消費行動を助けるサービス業者が当てはまる。

【００３４】

電子行政群４９は、たとえば市役所や税務署あるいは中央官庁等の行政を電子化したものである。ＸＭＬストア５０とは、ＸＭＬによる統一されたデータ構造によってデータを格納するとともに、必要に応じてデータの要求者に所定のデータを提供するデータベースのことである。ＸＭＬストア５０には、ユーザの各種個人情報やユーザエージェント（エージェント用知識データを含む）を格納している。金融機関群７やユーザからＸＭＬストア５０にアクセスがあった場合には、本人認証を行なってセキュリティを保ったうえで、必要なデータを提供できるように構成されている。コンテンツプロバイダ群５１とは、映像、文字、音等の種々のコンテンツをネットワークを通じて提供する業者群のことである。交通整理を行なうための信号機５２も、広域・大容量中継網４３に接続され、遠隔制御できるように構成されている。

【００３５】

携帯電話網４５に接続されている基地局５５に対し、ブラウザフォン（携帯電話）３０の電波が送信され、基地局５５，携帯電話網４５，ゲートウェイ５３，広域・大容量中継網４３を介して、金融機関群７，加盟店群６，ＮＭ群４８，電子行政群４９，ＸＭＬストア５０，コンテンツプロバイダ群５１等にアクセスできるように構成されている。また車両５６も同様に、基地局５５，携帯電話網５４，ゲートウェイ５３，広域・大容量中継網５４を介して、各種サービス業者や各種機関にアクセスできるように構成されている。

【００３６】

認証局群４６とは、電子証明書の発行希望者に対して本人認証をしたうえで電子証明書を発行する機関である。データセンタ４４は、放送局４１から電波により配信される各種データを格納，管理する機関のことである。加盟店群６，サプライヤ群Ｓ，ＮＭ群４８，電子行政群４９，コンテンツプロバイダ群５１等にユーザが所定の情報の送信を依頼した場合に、大容量のデータを送信する際には、それら各機関やサービス業者の配信するデータを一旦データセンタ４４に格納しておき、所定の日時が来たときに放送局４１から電波を通じてそのデータを配信し、受信局４２で受信したデータを所定のユーザに広域・大容量中継網４３を通じて配信する。

【００３７】

８はライフ支援センターである。このライフ支援センター８は、ユーザの個人情報を収集し、その個人情報に基づきユーザにふさわしい夢，人生設計，職種，趣味等を推薦して、それらを実現するために必要となる各種商品や情報を提供してくれる加盟店（ニューミドルマンを含む）を推薦するサービスを行なう機関である。

【００３８】

なお、図１中二重線で示した部分は、無線ＬＡＮ，ＣＡＴＶ，衛星，ｘＤＳＬ（digital sub scriber line），ＦＴＴＨ（fiber to the home）などである。

【００３９】

本実施の形態では、認証局群４６ばかりでなく、金融機関群７も、電子証明書を発行する。図１中、１９はユーザに携帯されるＩＣ端末であり、後述するようにユーザのプロフィール情報（個人情報）等が格納されている。

【００４０】

図２は、金融機関７を説明するための説明図である。金融機関７には、ＶＰ管理サーバ９、決済サーバ１０、認証用サーバ１１、データベース１２ａ，１２ｂが備えられている

。ＶＰ管理サーバ９は、仮想人物としてのバーチャルパーソン（以下、単に「ＶＰ」という）を管理するためのサーバである。ＶＰとは、現実世界に実在しないネットワーク上等で行動する仮想の人物のことであり、現実世界での実在人物であるリアルパーソン（以下、単に「ＲＰ」という）がネットワーク上等で行動する際に、ＶＰになりすましてそのＶＰとして行動できるようにするために誕生させた仮想人物のことである。また、後述するように、ＲＰが、ネットワーク上で行動するときばかりでなく、現実世界で行動するときにもＶＰになりすましてそのＶＰとして行動する場合がある。

【００４１】

ＶＰ管理サーバ９は、後述するように、ＲＰからＶＰの出生依頼があれば、そのＶＰの氏名や住所等の所定情報を決定してＶＰを誕生させ、そのＶＰのデータをデータベース１２ａに記憶させておく機能を有している。また、このＶＰ管理サーバ９は、ＶＰ用の電子証明書を作成して発行する機能も有している。ＶＰが売買や決済等の法律行為を行なう場合に、この電子証明書を相手方に送信することにより、仮想人物でありながら独立して法律行為を行なうことが可能となる。

【００４２】

認証用サーバ１１は、ＲＰ用の電子証明書を作成して発行する機能を有する。金融機関７に設置されている決済サーバ１０は、ＲＰによる電子マネーやデビットカードを使用しての決済ばかりでなく、ＶＰとして電子マネーやデビットカードを使用しての決済を行なうための処理を行なう機能も有している。

【００４３】

データベース１２ａは、ＲＰやＶＰに関するデータを格納するものである。データベース１２ｂは、広域・大容量中継網４３やインターネットＩに接続されているサイト（業者）を管理するためのデータを格納している。

【００４４】

図２に示すように、データベース１２ａには、ＲＰ用のデータとして、ＲＰの氏名、住所、認証鍵ＫＮ、公開鍵ＫＴ、口座番号等が記憶されている。認証鍵とは、ＲＰが金融機関７にアクセスしてきた場合に共通鍵暗号方式により本人認証を行なうための鍵である。公開鍵とは、公開鍵暗号方式に用いられる鍵であり、秘密鍵とペアとなっている鍵である。口座番号は、当該金融機関７においてＲＰが開設している口座番号のことである。

【００４５】

トラップ情報とは、サイト（業者）側が個人情報を収集してそれを不正に流通させた場合に、それを行なった犯人を割出すためにトラップ（罠）を仕掛けるための情報である。たとえば、ＶＰが自己の個人情報をある業者（第１譲渡先）に譲渡する際に、その第１譲渡先特有の氏名を用いる。すなわち、ＶＰが自己の氏名を複数種類有し、サイト（業者）ごとに使い分ける。このようなＶＰ氏名を、便宜上トラップ型ＶＰ氏名という。このようにすれば、ダイレクトメールやＥメールが業者側から送られてきた場合には、そのメールの宛名がトラップ型ＶＰ氏名となっているはずである。その送ってきたサイト（業者）が、トラップ型ＶＰ氏名から割出される第１譲渡先とは異なりかつ譲渡した自己の個人情報の開示許容範囲（流通許容範囲）を超えたサイト（業者）であった場合には、その個人情報が第１譲渡先によって不正に開示（流通）されたこととなる。このように、不正流通（不正開示）を行なった第１譲渡先を、トラップ型ＶＰ氏名から割出すことができる。

【００４６】

なお、図２では、次郎が第２トラップ情報、第３トラップ情報、第２個人情報、第３個人情報、２つの情報を有している。次郎が、ネットワーク上で行動する場合に、この２人のＶＰを使い分けて行動するために、これら２種類のＶＰ情報を金融機関７に登録している。ＶＰの住所とは、後述するように、ＲＰの希望するまたはＲＰの住所に近いコンビニエンスストア２の住所である。その結果、ＶＰとして電子ショッピングをした場合の商品の配達先が、そのＶＰの住所であるコンビニエンスストア２に配達されることとなる。ＲＰは、その配達されてきた商品をＶＰになりすましてコンビニエンスストア２にまで出向いて商品を引取ることが可能となる。このようにすれば、住所を手がかりにＶＰとＲＰと

の対応関係が見破られてしまう不都合が防止できる。

【００４７】

図２に示したトラップ情報の詳細は、図３に示されている。第１トラップ情報、第２トラップ情報、…の各トラップ情報は、サイト名（業社名）ごとに、氏名（トラップ型ＶＰ氏名）、公開鍵、Ｅメールアドレス、バーチャル口座番号、バーチャルクレジット番号を含んでいる。たとえば、サイト名（業者名）ＡＢＣにＶＰがアクセスする際には、ＶＰの本名であるＢ１３Ｐを用い、ＶＰの秘密鍵ＫＳＢとペアの公開鍵ＫＰＢ'を用い、ＶＰの本当のＥメールアドレスである○□×△×を用い、ＶＰの本当の口座番号である２５０３を用い、ＶＰの本当のクレジット番号である３２８８を用いる。

【００４８】

一方、サイト名（業者名）ＭＴＴにアクセスする（ＭＴＴで図３０の自動決済を行う）場合には、ＶＰの本名をそのＶＰの秘密鍵で１回暗号化したＥ（Ｂ１３Ｐ）を、トラップ型ＶＰ氏名として用いる。秘密鍵としては、ＶＰの本当の秘密鍵ＫＳＢをＶＰの本当の秘密鍵ＫＳＢで１回暗号化したＥＫＳＢ（ＫＳＢ）を用いる。この秘密鍵ＥＫＳＢ（ＫＳＢ）に対する公開鍵ＫＰＢがデータベース１２ａに格納されている。Ｅメールアドレスとしては、金融機関７がトラップ型ＶＰのために開設しているＥメールアドレス△△△△△を用いる。口座番号としては、ＶＰの本当の口座番号をＶＰの本当の秘密鍵で１回暗号化したＥ（２５０３）をバーチャル口座番号として用いる。クレジット番号は、ＶＰの本当のクレジット番号をＶＰの本当の秘密鍵で１回暗号化したＥ（３２８８）を用いる。

【００４９】

さらに、サイト名（業者名）ＭＥＣにアクセスする（ＭＥＣで図３０の自動決済を行う）場合には、ＶＰの秘密鍵でＶＰの本名を２回暗号化したＥ２（Ｂ１３Ｐ）をトラップ型ＶＰ氏名として用いる。

【００５０】

ＶＰがトラップ型ＶＰ氏名Ｅ２（Ｂ１３Ｐ）を用いてネットワーク上等で行動する場合には、秘密鍵ＫＳＢを秘密鍵ＫＳＢで２回暗号化した２回暗号化秘密鍵Ｅ２ＫＳＢ（ＫＳＢ）を用いる。その２回暗号化秘密鍵とペアになっている公開鍵がＫＰＢ″である。Ｅメールアドレスは、金融機関７がトラップ型ＶＰ用のＥメールアドレスとして開設している△△△△△を用いる。バーチャル口座番号は、ＶＰの本当の口座番号を秘密鍵で２回暗号化したＥ２（２５０３）を用いる。クレジット番号は、ＶＰの本当のクレジット番号をＶＰの秘密鍵で２回暗号化したバーチャルクレジット番号Ｅ２（３２８８）を用いる。

【００５１】

このように、サイト名（業社名）ごとに、トラップ情報の暗号回数が異なる。サイト側（業者側）に提供した個人情報というものは、ネットワーク上を流通した後最終的にはその個人情報主にＥメールやダイレクトメールの形で返ってくる。この個人情報の帰還ループを利用してトラップを仕掛けて個人情報の不正流通を行なった犯人を追跡できるようにするのが、このトラップ情報の狙いである。すなわち、ユーザをネット上で追跡するトラッキング型クッキーの逆を行なうものである。

【００５２】

図４は、図２に示したＶＰの個人情報を説明する図である。第１個人情報、第２個人情報、第３個人情報、…の各個人情報は、個人情報Ａ、個人情報Ｂ、…の複数種類の個人情報が集まって構成されている。たとえば、個人情報Ａは、ＶＰの年齢，性別，職業，年収等であり、個人情報Ｂは、ＶＰの嗜好に関する情報である。

【００５３】

図４に示すように、各個人情報は，金融機関７の秘密鍵ＫＳによるデジタル署名が付されている。たとえば，第１個人情報の個人情報Ａは、○○△の個人情報自体に対しデジタル署名であるD_{KS}（○○△）が付されている。

【００５４】

このデータベース１２ａに格納されている各個人情報は、後述するように、金融機関７がその真偽をチェックして正しいもののみをデータベース１２ａに格納し、正しいことを

認証するためのデジタル署名が付される。

【００５５】

図５は、ＸＭＬストア５０の構成を示す図である。ＸＭＬストア５０には、データベース７２とそれを制御するサーバ７１とが設置されている。サーバ７１は、ＸＭＬストア５０にアクセスしてきた者を、本人認証してアクセス制御する機能も備えている。

【００５６】

データベース７２には、ＸＭＬで表現されたデータが格納されている。そのデータの中身は、ＶＰ情報として、ＶＰの氏名であるたとえばＢ１３Ｐ、ＶＰユーザエージェント（知識データを含む）、サイト（業社）別情報として、サイト名（業社名）たとえばＡＢＣ、そのサイト（業社）にアクセスしたＶＰに発行された電子証明書、そのＶＰの個人情報と当該サイト（業社）のプライバシーポリシーとそれら両情報に対し当該ＶＰが付したデジタル署名D_{KSB}（個人情報＋ポリシー）と当該サイト（業社）ＡＢＣが付したデジタル署名D_{KSA}（個人情報＋ポリシー）と、トラップ情報としての暗号化回数「０」と、当該ＶＰのＥメールアドレスである○□×△×が含まれている。さらに、ＶＰがサイト名（業社名）ＭＴＴにアクセスした場合には、そのサイト名（業社名）ＭＴＴにアクセスしたトラップ型ＶＰに対し発行された電子証明書と、そのサイト（業社）にトラップ型ＶＰが提供した個人情報とそのサイト（業社）のプライバシーポリシーとそれら両情報に対する当該トラップ型ＶＰのデジタル署名と当該サイト（業社）のデジタル署名と、トラップ情報としての暗号回数「１」とＥメールアドレスとが含まれている。

【００５７】

さらに、氏名がＮＰＸＡの他のＶＰの情報も、前述と同様の項目がデータベース７２に記憶される。このデータベース７２には、非常に多くのＶＰごとに、前述した項目でデータが記憶されている。

【００５８】

なお、サイト名（業社名）ＡＢＣについては、図３で説明したように、トラップ情報として１回も暗号化していない情報を用いているために、データベース７２に格納されている暗号回数も「０」となっている。サイト名（業社名）ＭＴＴについて言えば、図３で説明したように、トラップ情報として１回暗号化した情報を用いているために、データベース７２に記憶されている暗号化回数も「１」となっている。

【００５９】

前述したＶＰユーザエージェントとは、ユーザであるＶＰのために動作する自立型ソフトウェアのことである。このＶＰユーザエージェントは、ネットワークを通して移動できるようにモバイルエージェントで構成されている。

【００６０】

なお、図２～図５に示した各データは、暗号化した状態で各データベースに格納しておいてもよい。そうすれば、万一データが盗まれたとしても、解読できないために、セキュリティ上の信頼性が向上する。一方、たとえばＶＰ（トラップ型ＶＰを含む）がネットワーク上で目に余る不正行為（たとえば刑法に違反する行為）を行なった場合には、所定機関（たとえば警察等）からの要請等に応じて、そのＶＰをデータベース１２ａ等から検索してそのＶＰに対応するＲＰを割出し、ＲＰの住所氏名等を要請のあった所定機関（たとえば警察等）に提供するようにしてもよい。

【００６１】

図６は、コンビニエンスストア２の構成を示す図である。コンビニエンスストア２には、データベース７５と、それに接続されたサーバ７４と、そのサーバに接続された端末７３とが設置されている。データベース７５には、当該コンビニエンスストアに住所を持つＶＰ（トラップ型ＶＰを含む）の氏名と、それら各氏名に対応して、商品の預かり情報、Ｅメールアドレス、顧客管理情報等が記憶されている。

【００６２】

当該コンビニエンスストア２にＢ１３ＰのＶＰが購入した商品が配達されれば、データベース７５のＢ１３Ｐの記憶領域に、商品預かり情報として「ＡＢＣ会社からの商品預か

り，未決済」が格納される。この未決済とは、Ｂ１３Ｐがネットを通じて商品を購入したもののまだ支払を行なっていない状態のことである。

【００６３】

データベース７５のＥメールアドレスの欄には、各ＶＰに対応してＥメールアドレスが格納されている。Ｂ１３Ｐの場合には、トラップ型ＶＰでないために、当該ＶＰの本当のＥメールアドレスである○□×△×が格納されている。

【００６４】

トラップ型ＶＰであるＥ（Ｂ１３Ｐ）も同様に、商品預かり情報としてたとえば「ＭＴＴ会社からの商品預かり，決済済」が格納される。なお、Ｅ（Ｂ１３Ｐ）は、トラップ型ＶＰであるために、Ｅメールアドレスは、金融機関７のトラップ型ＶＰのために開設されているＥメールアドレスが格納される。

【００６５】

サーバ７４は、後述するように、コンビニエンスストア２にＶＰ（トラップ型ＶＰを含む）として商品を引取りに来た顧客が、当該コンビニエンスストア２に登録されているＶＰ（トラップ型ＶＰを含む）に対し商品を預かっている場合にはその商品をＶＰ（トラップ型ＶＰを含む）に引渡すための処理を行なう。

【００６６】

コンビニエンスストア２は、商品の預かりサービスばかりでなくＶＰ用のダイレクトメールの預かりサービスも行なう。ＶＰはコンビニエンスストア２が住所でありＶＰ宛のダイレクトメールはコンビニエンスストア２に郵送されるためである。

【００６７】

図７は、ユーザに用いられる端末の一例のブラウザフォン３０を示す正面図である。ブラウザフォン３０には、マイクロコンピュータ１９９が備えられている。このマイクロコンピュータ１９９には、ＣＰＵ（Central Processing Unit）１９７と、Ｉ／Ｏポート１９８と、ＲＯＭ１９５と、ＥＥＰＲＯＭ１９４と、ＲＡＭ１９６とが備えられている。このブラウザフォン３０は、ＵＳＢ（Universal Serial Bus）ポートを備えており、ＵＳＢポートに対し、ＩＣ端末１９Ｒまたは１９Ｖまたは１９Ｉが差込み可能に構成されている。ＩＣ端末１９Ｒは、ＲＰ用のＩＣ端末である。ＩＣ端末１９Ｖは、ＶＰ用のＩＣ端末である。ＩＣ端末１９Ｉは、後述するように金融機関が発行したＶＰ用のデータやプログラムが格納されてユーザにまで配達されてくるものであり、その配達されてきたＩＣ端末１９ＩをブラウザフォンのＵＳＢポートに指込むことにより、ＩＣ端末１９Ｉに記憶されているデータやソフトウェアがブラウザフォン３０に記憶されることとなる。なお、各ＩＣ端末１９Ｒ，１９Ｖ、１９Ｉは、ＩＣカードで構成してもよい。

【００６８】

図８は、ＶＰ用ＩＣ端末１９Ｖを説明するための説明図である。ＶＰ用ＩＣ端末１９Ｖは、前述したように、ブラウザフォン３０のＵＳＢポート１８に対し着脱自在に構成されており、ＵＳＢポート１８に差込むことにより、ブラウザフォン３０との情報がやり取りできるようになり、使用可能な状態となる。

【００６９】

ＶＰ用ＩＣ端末１９Ｖ内には、ＬＳＩチップ２０が組込まれている。このＬＳＩチップ２０には、制御中枢としてのＣＰＵ２４、ＣＰＵ２４の動作プログラムが記憶されているＲＯＭ２５、ＣＰＵ２４のワークエリアとしてのＲＡＭ２２、電気的に記憶データを消去可能なＥＥＰＲＯＭ２６、コプロセッサ２３、外部とのデータの入出力を行なうためのＩ／Ｏポート２１等が設けられており、それらがバスにより接続されている。

【００７０】

ＥＥＰＲＯＭ２６には、電子マネー用のプログラムであるモンデックス（リロード金額データを含む）、その他の各種アプリケーションソフト、ＶＰ用に発行された電子証明書、暗証番号、トラップ型ＲＦＩＤが記憶されている。このトラップ型ＲＦＩＤとは、ユーザがトラップ型ＶＰとして行動する際にそのトラップ型ＶＰに対応するＲＦＩＤを発信するために記憶しているＲＦＩＤである。詳しくは後述する。

【００７１】
さらに、ＶＰ用ＩＣ端末１９Ｖは、ＶＰのユーザエージェントとしての機能を有しており、ユーザエージェント用知識データとして、デビットカード情報、クレジットカード情報、ＶＰの氏名，住所、ＶＰのＥメールアドレス、ＶＰの公開鍵ＫＰと秘密鍵ＫＳ、ＲＰの認証鍵ＫＮ、ＶＰの年齢，職業等、ＶＰの各種嗜好情報、ＶＰの家族構成、…等の各種知識データが記憶されている。
【００７２】
ＲＰ用ＩＣ端末１９Ｒの場合も、図８に示したＶＰ用ＩＣ端末１９Ｖとほぼ同様の構成を有している。相違点といえば、ＥＥＰＲＯＭ２６に記録されているユーザエージェント用知識データの内容が相違する。具体的には、ＶＰの氏名，住所の代わりにＲＰの氏名，住所、ＶＰのＥメールアドレスの代わりにＲＰのＥメールアドレス，ＶＰの公開鍵や秘密鍵の代わりにＲＰの公開鍵，秘密鍵、ＶＰの年齢や職業等の代わりにＲＰの年齢や職業等、ＶＰの各種嗜好情報の代わりにＲＰの各種嗜好情報、ＶＰの家族構成の代わりにＲＰの家族構成となる。トラップ型ＲＦＩＤは記憶していない。
【００７３】
なお、ＶＰの家族構成は、ＶＰに対応するＲＰの家族がＶＰを誕生させている場合には、その誕生しているＶＰの名前や住所や年齢等のデータから構成されている。つまり、ＲＰの家族に対応するＶＰの家族すなわちバーチャル家族のデータがこのＶＰの家族構成の記憶領域に記憶されることとなる。
【００７４】
図９は、図８に示したトラップ型ＲＦＩＤの詳細を示す図である。トラップ型ＲＦＩＤの記憶領域には、ＶＰ氏名ごとに、そのＶＰ氏名に対応するトラップ型ＲＦＩＤが格納される。たとえば量販店等の業社ＮＴＴでＶＰとしてポイントカード等を作成する際にＶＰがトラップ型ＶＰ名Ｅ（Ｂ１３Ｐ）を登録した場合には、その業社でショッピング等の行動を行なう際にＥ（Ｂ１３Ｐ）に対応するトラップ型ＲＦＩＤであるｍｔｔをブラウザフォン（携帯電話）３０から発信する。そのために各トラップ型ＶＰに対応させてトラップ型ＲＦＩＤを記憶させている。たとえば、業社ＭＴＴ内でショッピング等の行動を行なう際にＥ（Ｂ１３Ｐ）に対応するトラップ型ＲＦＩＤであるｍｔｔをブラウザフォン（携帯電話）３０から発信し、トラップ型ＶＰ名E^2（Ｂ１３Ｐ）を登録している業社ＭＥＣ内でショッピング等の行動を行なう際同じｍｔｔをブラウザフォン（携帯電話）３０から発信した場合には、ＲＦＩＤｍｔｔを手がかりにＥ（Ｂ１３Ｐ）とE^2（Ｂ１３Ｐ）とは同一人物であることが見破られてしまう虞がある。このような不都合を防止するために、業社毎に発信するＲＦＩＤを異ならせる。
【００７５】
また、たとえば業社ＭＴＴ内でショッピング等の行動を行なう際にＥ（Ｂ１３Ｐ）に対応するトラップ型ＲＦＩＤであるｍｔｔをブラウザフォン（携帯電話）３０から発信し、かつ、ＶＰ名等の個人情報を一切登録していない小売店ＡＭＰＭでショッピング等の行動をする際にｍｔｔを発信し、後日小売店ＡＭＰＭから電子メールまたはダイレクトメールがＥ（Ｂ１３Ｐ）宛に送られてきた場合には、Ｅ（Ｂ１３Ｐ）の個人情報が業社ＭＴＴから小売店ＡＭＰＭに不正に横流しされたことになる。そのような横流しを監視することができる。
【００７６】
なお、ＩＣ端末１９Ｖ，１９ＲのＥＥＰＲＯＭ２６には、公開鍵ＫＰ、秘密鍵ＫＳ、認証鍵ＫＮ、暗証番号のみを記憶させ、それ以外の情報はすべてＸＭＬストア５０の方に記憶させて必要に応じて検索して利用できるようにしてもよい。また、公開鍵ＫＰ、秘密鍵ＫＳを用いた暗号化や復号処理は、ＩＣ端末１９Ｖ，１９Ｒ自体が行うのではなく、ブラウザフォン３０あるいは後述するパーソナルコンピュータ３０’が行うようにしてもよい。その場合には、公開鍵ＫＰ、秘密鍵ＫＳをブラウザフォン３０あるいは後述するパーソナルコンピュータ３０’に出力する必要がある。
【００７７】

図１０は、携帯装置１の機能の概略を示すブロック図である。図４を参照して、携帯装置１は、たとえば指輪の形状をしており、ユーザの身体に装着しやすい形状となっている。以下、携帯装置１をＩＤリング１という。ＩＤリング１は、入浴や就眠時も常時身につけることを原則とし、このことにより紛失や盗難を防ぐことができる。また、ＩＤリング１にはセキュリティ用のＲＦＩＤタグ１ａが設けられており、そのＲＦＩＤタグ１ａは、ＲＦＩＤタグ１ａの全体を制御するためのロジック（ＣＰＵ）１００と、暗号化されたＲＦＩＤを記憶するための読出し専用メモリ（ＲＯＭ：Read Only Memory）１０１と、ロジック１００で実行する際に必要なランダムアクセスメモリ（ＲＡＭ：Random AcceＳＳ Memory）１０２と、電気消去可能プログラマブル読出し専用メモリ（ＥＥＰＲＯＭ：electrically erasable programmable read-only memory）１０３と、電源に用いられる電波を受信し、信号を送受信するためのループアンテナ１０７ａ、１０７ｂと、受信された電源に用いられる電波から電力を発生するための電源制御部１０６と、受信した信号を復調し、送信するための信号を変調するための変調・復調部１０５と、変調・復調部１０５への信号の入出力を制御するための入出力制御部１０４とを含む。ロジック１００、ＲＯＭ１０１、ＲＡＭ１０２、ＥＥＰＲＯＭ１０３、入出力制御部１０４は、それぞれデータバス１０８によって接続されている。

【００７８】

ロジック１００は、ＲＯＭ１０１、ＲＡＭ１０２、ＥＥＰＲＯＭ１０３、入出力制御部１０４を制御して、後述する各種処理を実行する。

【００７９】

ＲＯＭ１０１は、ＲＦＩＤタグ１ａに付され、他のＲＦＩＤタグ１ａと識別するためのＲＦＩＤとを記憶する。ＲＦＩＤは、ＲＦＩＤタグ１ａが製造される段階、または、ユーザに発行される前の段階で記録され、その後消去されることはない。

【００８０】

ＥＥＰＲＯＭ１０３には、ブラウザフォン３０から送信されてきた本人認証用のパスワードが記憶される。後述するようにＲＦＩＤタグ１ａを一旦発信停止状態にした後発信を再開できる状態にするときに、ブラウザフォン３０からパスワードが送信され、その送信されてきたパスワードを予めＥＥＰＲＯＭ１０３に記憶されているパスワードと照合し一致すると判断された場合にのみ、ＲＦＩＤタグ１ａがＲＦＩＤを発信できる状態に切換わる。

【００８１】

入出力制御部１０４は、ＣＰＵ１００により制御され、変調・復調部１０５およびループアンテナ１０７ａを介して情報を送受信する。これにより、ＲＦＩＤタグ１ａは、スキャナ（ＲＦＩＤタグリーダライタ）２０１と無線による通信が可能である。ＲＦＩＤタグ１ａとスキャナ２０１との間の通信は、非接触型のＩＣカードを用いた場合の通信と同様の技術が用いられる。したがって、ここではその詳細な説明は繰返さない。

【００８２】

一方のループアンテナ１０７ｂには大容量のコンデンサ１１０が接続されており、電源に用いられる電波をこのループアンテナ１０７ｂが受信してコンデンサ１１０に電力を貯えるように構成されている。電源に用いられる電波の送信が停止したときにこのコンデンサ１１０に貯えられている電力を電源制御部１０６に供給して引き続き所定時間（たとえば１０秒程度）ＲＦＩＤタグ１ａが作動できるように構成されている。

【００８３】

図１１は、図１０に示したＲＦＩＤタグ１ａのロジック（ＣＰＵ）１００の制御動作を示すフローチャートである。先ずＳＡ１により、ＲＦＩＤ送信指令を受信したか否かの判断がなされ、受信するまで待機する。タグリーダから電源用の電波が発せられて静電誘導によりループアンテナ１０７ａに電力が発生した状態でロジック１００が動作可能となり、その状態でタグリーダから送信されてきたＲＦＩＤ送信指令をループアンテナ１０７ａが受信すれば、ＳＡ１によりＹＥＳの判断がなされてＳＡ２へ進み、前回のＲＦＩＤ発信から５秒経過したか否かの判断がなされる。５秒経過していない場合にはＳＡ１０により

、前回発信したＲＦＩＤと同じものを発信する処理がなされる。５秒経過している場合には、ＳＡ３へ進み、ランダムカウンタのカウント値ＲをＥＥＰＲＯＭ１０３から読出す（抽出する）処理がなされる。このランダムカウンタは、偽ＲＦＩＤのコードをランダムに生成するためのカウンタであり、後述するＳＡ７～ＳＡ９により数値データが更新される。

【００８４】

次に制御がＳＡ４へ進み、抽出したカウント値Ｒに基づいてテーブルを参照し、偽ＲＦＩＤを割出す処理がなされる。ＳＡ４により参照されるテーブルが、図１２に示されている。図１２は東京都千代田区（図１３参照）で販売されるＲＦＩＤタグ１ａのテーブルを示しており、（ａ）は、１回で１つのＲＦＩＤを発信する単数発信タイプのＲＦＩＤタグ１ａが記憶しているテーブルである。図１２（ｂ）、（ｃ）は、１度に複数（例えば４個）の偽ＲＦＩＤを発信する複数発信タイプのＲＦＩＤタグに記憶されているテーブルである。この複数発信タイプのＲＦＩＤタグは、複数種類製造されて販売される。そのうちの２種類のＲＦＩＤタグ１ａに記憶されているテーブルを図１２（ｂ）（ｃ）に示す。複数発信タイプのＲＦＩＤタグは、図１２（ｂ）（ｃ）からも分かるように、ランダムカウンタの抽出値（乱数）が０～３９の範囲のときに検索される４つの偽ＲＦＩＤ１～４のうち３つの偽ＲＦＩＤ２～４が互いに共通のコードとなっており、１つのＲＦＩＤ１のみ互いに異なるように構成されている。また、ランダムカウンタの抽出値（乱数）が０～３９以外の範囲のときに検索される４つの偽ＲＦＩＤ１～４は、互いに異なるバラバラなコードとなっている。一方、単数発信タイプのＲＦＩＤタグも複数種類製造販売され、ランダムカウンタの抽出値（乱数）が０～３９の範囲のときに検索される偽ＲＦＩＤが互いに共通のコードとなっており、ランダムカウンタの抽出値（乱数）が０～３９以外の範囲のときに検索される偽ＲＦＩＤが互いに異なるバラバラなコードとなっている。

【００８５】

前述したランダムカウンタは、ＳＡ７により「１」加算更新された後ＳＡ８によりその値が１００以上になったか否かの判断がなされ、なった場合にはＳＡ９によりランダムカウンタの値を「０」にする処理がなされる。その結果、ランダムカウンタは、０からカウントアップしてその上限である９９までカウントアップされたのち、再度０からカウントアップし直すように構成されており、このようなランダムカウンタが数値データを抽出すれば、０～９９の範囲内の任意の値（乱数）が抽出されることとなる。図１２（ａ）のテーブルを記憶している単数発信タイプのＲＦＩＤタグ１ａの場合には、抽出したカウント値（乱数）Ｒに基づいてそのテーブルを参照し、例えば抽出したランダムカウンタの値Ｒが０～３９の範囲内の値であった場合には、８２０４９３１７６の偽ＲＦＩＤがＳＡ４により割出されることとなる。また、例えば抽出したランダムカウンタＲの値が５５～６９の範囲内の数値であった場合には、８１３９２６０８１の偽ＲＦＩＤがＳＡ４により割出されることとなる。同様に、図１２（b）に示されたテーブルを記憶している複数発信タイプのＲＦＩＤタグ１ａの場合には、例えば抽出したランダムカウンタＲの値が５５～６９の範囲内の数値であった場合には、８１４３５８２３１、８４９１３７６５５、７８８０１５２３３、７７９２８８４０１の偽ＲＦＩＤがＳＡ４により割出されることとなる。また、図１２（ｃ）に示されたテーブルを記憶している複数発信タイプのＲＦＩＤタグ１ａの場合には、例えば抽出したランダムカウンタＲの値が８５～９９の範囲内の数値であった場合には、７００９１３５６１、７５００２１２１４、７０２０４９３１９、８５６１０４９２３の偽ＲＦＩＤがＳＡ４により割出されることとなる。

【００８６】

次に制御がＳＡ５へ進み、その割出された偽ＲＦＩＤをループアンテナ１０７ａから発信する処理がなされる。

【００８７】

単数発信タイプのＲＦＩＤタグ１ａのそれぞれは、４０％の確率で８２０４９３１７６の共通偽ＲＦＩＤを発信し（図１２（ａ）参照）、かつそれぞれ１５％の確率で、７３０８５４７０９の偽ＲＦＩＤ、８１３９２６０８１の偽ＲＦＩＤ、７９１４０５７３１の偽

ＲＦＩＤ、８３５４０６９１２等の互いにバラバラな偽ＲＦＩＤを発信することとなる。その結果、このようなＲＦＩＤタグ１ａを複数の個人ユーザが身に付けておれば、毎回ランダムなコードからなる偽ＲＦＩＤが発信されるものの、４０％という１番発信確率の高い８２０４９３１７６の偽ＲＦＩＤ（以下「共通偽ＲＦＩＤ」という）が頻繁に発信されることとなる。その結果、異なった複数場所に設置されたタグリーダによって読取られたＲＦＩＤがたまたま同一コードのＲＦＩＤであった場合には、本来なら同一人物から発信されたＲＦＩＤと判断できるが、このＲＦＩＤタグ１ａが複数の個人ユーザに所持されることにより、複数箇所で同一のＲＦＩＤを受信したとしてもそれが異なる人物によって発信された前記共通偽ＲＦＩＤである可能性も生じる（異人物同一識別子発信現象）。その結果、同一のＲＦＩＤを複数箇所で受信したとしても必ずしも同一人物であるとは限らないこととなり、悪意のＲＦＩＤ受信者側の同一人物である旨の推測を撹乱することができ、個人ユーザのプライバシーを保護することができる。

【００８８】

図１２（ａ）に示すテーブルを記憶した単数発信タイプのＲＦＩＤタグ１ａのみの場合には、そのＲＦＩＤタグ１ａを所持する個人ユーザが他にＲＦＩＤタグを一切所持していないかあるいは所持してもＲＦＩＤ発信停止状態にしている場合には、前述した撹乱効果が有効に発揮される。しかし、個人ユーザが身に付けている複数の商品それぞれに付されているＲＦＩＤタグからＲＦＩＤが発信される状態となっている場合には、単数発信タイプのＲＦＩＤタグ１ａを所持している状態では、タグリーダからのＲＦＩＤ送信指令が発せられれば、ＲＦＩＤタグ１ａからランダムな偽ＲＦＩＤが発せられるとともに、当該個人ユーザが所持している商品に付されているＲＦＩＤタグから毎回同じＲＦＩＤが発信されることとなる。その結果、同一人物が或る場所に設置されたタグリーダに対して複数のＲＦＩＤを発信した後他の場所へ移動してそこに設置されているタグリーダに対し複数のＲＦＩＤを発信した場合には、複数のＲＦＩＤの内の一つが異なり他のものがすべて同一という現象（複数識別子中１個可変型現象）が生ずる。ただし、偶然すべてのＲＦＩＤが一致する状態となることもまれにある。その結果、一度に複数のＲＦＩＤを受信した場合には、その内の１つのＲＦＩＤが異なり他の全てが一致するかまたは全てのＲＦＩＤが一致する場合には、同一人物であると推測されてしまう不都合が生ずる。

【００８９】

そこで、図１２（ａ）に示したテーブルを記憶している単数発信タイプのＲＦＩＤタグ１ａばかりでなく、図１２（ｂ）、（ｃ）に示すようなテーブルを記憶した複数発信タイプのＲＦＩＤタグ１ａも合わせて製造販売して個人ユーザに普及させる。

【００９０】

具体的には、購入済みの所持品に付されているＲＦＩＤタグを発信停止状態等にして自己の所持品からＲＦＩＤが他人に読取れないようにしている個人ユーザには、前述の複数発信タイプのＲＦＩＤタグ１ａを普及させる。一方、他人が購入済み商品からのＲＦＩＤを読取ることができるようになっている個人ユーザに対しては、前述の単数発信タイプのＲＦＩＤタグ１ａを提供する。前者の個人ユーザの場合には、前述したように、１つの偽ＲＦＩＤがランダムに発信されるとともに所持品に付されているＲＦＩＤタグから本物のＲＦＩＤが同時に発信されるという現象（複数識別子中１個可変型現象）が生ずる。一方、後者の個人ユーザの場合には、１度に複数（図１２の場合には４個）の偽ＲＦＩＤ１～４がランダムに発信される状態となる。ところが、前述したように、個人ユーザ同士の間で、４０％の確率で共通偽ＲＦＩＤ２～４と１つの異なったＲＦＩＤ１とが発信される状態となる。このような現象は、前述の複数識別子中１個可変型現象と同じ現象であるが、異なった人物の間でこの複数識別子中１個可変型現象が生ずることとなる。その結果、悪意の受信者側にしてみれば、複数識別子中１個可変型現象が生ずれば同一人物であるという推測の信頼性が低下するととととなり、同一人物の推測に基づいたプライバシーの侵害が前提から崩れることとなる。

【００９１】

次に図１１に戻り、ＳＡ６により電圧低下が生じたか否かの判断がなされる。これは、

電力用の電波の発信が停止して大容量のコンデンサ１１０に貯えられている電力を使用してＲＦＩＤタグ１ａが作動している状態で、そのコンデンサ１１０の貯留電力か少なくなってロジック１００に供給される電圧が低下したか否かを判別するものである。電圧が低下したと判別された場合には、ＳＡ１０ａに進み、現時点のランダムカウンタのカウント値ＲがＥＥＰＲＯＭ１０３に記憶された後この偽ＲＦＩＤタグの動作がストップする。このＳＡ１０ａにより記憶されたランダムカウンタのカウント値ＲがＳＡ３により読出される（抽出される）。一方、電源用の電力が供給されている最中あるいは電源用電力がストップした後コンデンサ１１０から充分電力が供給されている最中には、ＳＡ６によりＮＯの判断がなされてＳＡ７以降のランダムカウンタの加算更新処理が実行されることとなる。

【００９２】

図１３は、前述した複数種類の偽ＲＦＩＤタグ１ａをグループ分けしてそのグループ毎に地域を指定して販売する地域指定方式の一例を示す説明図である。図１３（ａ）は、図１２（ａ）のテーブルを記憶している単数発信タイプのＲＦＩＤ１ａの地域指定の一例を示し、図１３（ｂ）は、図１２（ｂ）（ｃ）に示された複数発信タイプのＲＦＩＤタグ１ａの地域指定の一例を示す図である。

【００９３】

図１２（ａ）に示された８２０４９３１７６を共通偽ＲＦＩＤとして発信可能なグループに属する単数発信タイプのＲＦＩＤタグ１ａは、図１３（ａ）に示すように、東京都千代田区で販売される。また、他のグループに属する８０９２０７３２１を共通偽ＲＦＩＤとして発信するグループに属する単数発信タイプのＲＦＩＤ１ａは、東京都新宿区で販売される。更に、例えば７９８０９１３２０を共通偽ＲＦＩＤとして発信するグループに属する単数発信タイプのＲＦＩＤタグ１ａは、京都市右京区で販売される。

【００９４】

一方、複数発信タイプのＲＦＩＤタグ１ａの場合には、図１２（ｂ）（ｃ）に示されたように、７７９２０３９８０，８３９０９３１２７，７４０９８０３４６の３種類の共通偽ＲＦＩＤを１度に発信するグループに属する複数発信タイプのＲＦＩＤタグ１ａは、東京都千代田区で販売される。また、他のグループに属する７８８７１８９５５，８４５５９０３２９，８２２７７０９４５を共通偽ＲＦＩＤとして発信するグループに属する複数発信タイプのＲＦＩＤタグ１ａは、京都市右京区で販売される。

【００９５】

尚、地域指定の販売方法としては、その地域内でその地域に対応するグループに属するＲＦＩＤタグ１ａを販売するのに限らず、販売時に使用地域（例えば千代田区、新宿区、右京区等）を表示して、個人ユーザが使用しようと思っている地域の表示を見て選択して購入する方法でもよい。

【００９６】

このように、地域を指定して個人ユーザに提供することにより、共通偽ＲＦＩＤが一致する同一グループに属するＲＦＩＤタグ１ａが極力同一地域内で使用されることとなり、同一地域内おいて同一の共通偽ＲＦＩＤが発信され易いという傾向が生じ、悪意のプライバシー侵害者を効果的に撹乱できる状態となる。

【００９７】

図１４は、ブラウザフォン３０の動作を説明するためのフローチャートである。Ｓ９５ａにより、ＲＦＩＤタグ切換処理がなされる。この処理は、個人ユーザが身に付けている購入済み商品に付されているＲＦＩＤタグを発信停止状態（識別子ガード状態）または発信再開状態に切換える処理である。Ｓ９５ｂにより、偽モード処理がなされる。この処理は、前述のセキュリティ用のＲＦＩＤタグ１ａの偽ＲＦＩＤ発信機能をブラウザフォン３０に持たせる処理である。Ｓ９５ｃにより、トラップモード処理がなされる。この処理は、個人ユーザが前述のトラップ型ＶＰとして自動決済等を行なう場合にそのトラップ型ＶＰに対応する偽ＲＦＩＤを発信するための処理である。Ｓ９５ｄにより、ＲＦＩＤ発信処理がなされる。この処理は、タグリーダからＲＦＩＤ発信要求があった場合にブラウザフ

ォン３０からＲＦＩＤを発信するための処理である。Ｓ９５により、ＩＣ端末使用モードであるか否かの判断がなされる。ブラウザフォン３０は、ＲＰ用ＩＣ端末１９ＲまたはＶＰ用ＩＣ端末１９Ｖのうちのいずれか少なくとも一方をＵＳＢポート１８に接続していなければ動作しないＩＣ端末使用モードと、ＩＣ端末を接続していなくても動作可能なＩＣ端末未使用モードとに切換えることが可能に構成されている。そして、ＩＣ未使用モードでない場合にはＳ９６へ進み、その他の処理がなされるが、ＩＣ端末使用モードになっている場合には、Ｓ９７へ進み、ＶＰ用ＩＣ端末１９Ｖが接続されているか否かの判断がなされ、接続されていない場合にはＳ９８へ進み、ＲＰ用ＩＣ端末１９Ｒが接続されているか否かの判断がなされ、接続されていない場合すなわち両ＩＣ端末ともに接続されていない場合には、制御はＳ９９へ進み、ＩＣ端末未使用の警告表示がなされた後Ｓ９５へ戻る。

【００９８】

一方、ＶＰ用ＩＣ端末１９Ｖが接続されている場合には、制御はＳ１００へ進み、自動決済処理がなされる。この処理については、図３１に基づいて後述する。次にＳ１００ａにより、ポイントカード登録処理がなされる。これは、百貨店等の業社においてポイントカードを新規発行してもらうための処理である。次に制御はＳ１０１へ進み、ＶＰ出生依頼処理がなされる。次にＳ１０２へ進み、ＶＰ用入力処理がなされる。次にＳ１０３へ進みＶＰ用決済処理がなされる。

【００９９】

次に制御がＳ５８０へ進み、個人情報の登録処理がなされる。この個人情報の登録処理は、図１８（ｂ）に示したＶＰ管理サーバ９の登録処理に対応するブラウザフォン３０側の処理である。まずＶＰとしての本人認証処理を行ない、ＶＰ管理サーバ９が本人認証の確認を行なったことを条件として、ＶＰの個人情報を金融機関７のＶＰ管理サーバ９へ送信してデータベース１２ａに登録してもらう処理を行なう。

【０１００】

次に制御がＳ５８２へ進み、個人情報の確認処理がなされる。この処理は、金融機関７のＶＰ管理サーバ９とブラウザフォン３０との間でなされる処理である。まずＶＰとしての本人認証がなされ、次に、データベース１２ａに格納されている自分の個人情報の確認を行なう処理がなされる。一方、確認の結果誤りがある場合あるいは引越しや転職等によって個人情報に変更があった場合には、このＳ５８２により、その変更情報が、金融機関７のＶＰ管理サーバ９へ送信される。

【０１０１】

次に制御がＳ５８３へ進み、商品検索・購入処理がなされる。この処理は、図４５に基づいて後述する。次に制御がＳ５８５へ進み、住所，氏名，Ｅメールアドレスの送信処理が行なわれる。一方、ブラウザフォン３０のＵＳＢポート１８にＲＰ用ＩＣ端末１９Ｒが接続されている場合には、Ｓ９８によりＹＥＳの判断がなされてＳ１０５へ進み、電子証明書発行要求処理がなされる。次に制御がＳ１０６へ進み、ＲＰ用入力処理がなされる。次にＳ１０７へ進み、ＲＰ用決済処理がなされる。この処理については、ＶＰ用決済処理と類似した制御処理である。

【０１０２】

図１５は、Ｓ９５ａに示したＲＦＩＤタグ切換え処理のサブルーチンプログラムを示すフローチャートである。ＳＢ１により、ＯＦＦ切換え操作があったか否かの判断がなされる。切換え操作がない場合にはＳＢ２へ進み、ＯＮ切換え操作があったか否かの判断がなされる。操作がない場合にはこのサブルーチンプログラムが終了する。

【０１０３】

一方、個人ユーザが所持している購入済み物品に付されているＲＦＩＤタグを発信停止状態にするためのＯＦＦ切換え操作がブラウザフォン３０によりなされた場合には、ＳＢ１によりＹＥＳの判断がなされてＳＢ３へ進み、そのブラウザフォン３０からパスワードが購入済み物品に付されているＲＦＩＤタグに発信される。ＲＦＩＤタグはその発信されてきたパスワードを記憶する。次にＳＢ４に従ってブラウザフォン３０からＯＦＦモード

指令が発信される。これを受けたＲＦＩＤタグは、記憶しているＲＦＩＤを発信しない状態に切換わる。これにより、ＲＦＩＤタグが、個人ユーザの意思に従って他人が読取れない識別子ガード状態になる。この識別子ガード状態の他の例としては、ＲＦＩＤタグをアルミ箔等で覆いＲＦＩＤを他人が読取れないようにするものであってもよい。また、ＲＦＩＤタグからのＲＦＩＤの読取りを妨害する妨害電波等を発信する装置を個人ユーザが携帯し、タグリーダからのＲＦＩＤ読取り要求があったときに妨害電波等を発信してＲＦＩＤを読取れないようにしてもよい。次にＳＢ５に従ってブラウザフォン３０からＲＦＩＤタグへ送信指令が発信される。次にＳＢ６へ進み、ＲＦＩＤの受信があったか否かの判断がなされる。ＳＢ４に従ってＯＦＦモード指令が既に発信されているために、通常では、個人ユーザに所持されている購入済物品に付されているＲＦＩＤタグからＲＦＩＤが発信されることはない。従って、ＳＢ６によりＮＯの判断がなされてＳＢ７によりＯＦＦモード切換え完了の表示がブラウザフォン３０によりなされる。ところが、ＳＢ４によりＯＦＦモード指令を発信したにもかかわらず、電波状況が悪かったり何らかの受信ミスが発信して個人ユーザに所持されている購入済み物品に付されているＲＦＩＤが発信停止状態に切換わらなかった場合には、ＳＢ６によりＹＥＳの判断がなされてＳＢ８に進み、ブラウザフォン３０によりエラー表示がなされる。

【０１０４】

個人ユーザに所持されている購入済物品に付されているＲＦＩＤタグがＲＦＩＤ発信停止状態になった後、それを再度発信再開状態に切換えるためのＯＮ切換え操作がブラウザフォン３０により行なわれた場合には、ＳＢ２によりＹＥＳの判断がなされてＳＢ９へ進み、本人認証用のパスワードが発信される。このパスワードを受信した個人ユーザの購入済物品に付されているＲＦＩＤタグは、記憶しているパスワードと照合して一致するか否かの判断を行なって本人認証を行なう。次にブラウザフォン３０は、ＳＢ１２に従って、ＮＯモード指令を発信する。これを受けた購入済物品に付されているＲＦＩＤタグは、前述したパスワードの照合によって本人認証が確認できたことを条件としてＯＮモード指令を受信することにより、ＲＦＩＤが発信可能な状態に切換わる。

【０１０５】

次にブラウザフォン３０から、ＳＢ１１にしたがってＲＦＩＤ送信指令が発信される。次にＳＢ１２により、ＲＦＩＤの受信があったか否かの判断がなされる。適正に本人認証の確認ができかつＯＮモード指令を受信しておれば購入済物品に付されているＲＦＩＤからＲＦＩＤが発信される。その場合には、ＳＢ１２によりＹＥＳの判断がなされてＳＢ１３お進み、ＯＮモード切変え完了表示がブラウザフォン３０によりなされる。一方、本人認証が確認できなかった場合やＲＦＩＤ送信指令の電波を受信し損なった場合には購入済み物品に付されているＲＦＩＤタグからＲＦＩＤが発信されない。その場合には、ＳＢ１２よりＮＯの判断がなされてＳＢ８へ進み、ブラウザフォン３０によりエラー表示がなされる。

【０１０６】

図１６は、個人ユーザに所持されている購入済み物品に付されているＲＦＩＤタグの動作を示すフローチャートである。ＳＣ１により、パスワードを受信したか否かの判断がなされ、受信していない場合にはＳＣ２へ進み、ＲＦＩＤ送信指令を受信したか否かに判断がなされ、受信していない場合にはＳＣ１へ戻る。このＳＣ１→ＳＣ２→ＳＣ１のループの巡回途中でＳＢ３またはＳＢ９にしたがってブラウザフォン３０からパスワードが発信されてくれば、ＳＣ１によりＹＥＳの判断がなされてＳＣ３へ進む。ＳＣ３では、OFFモード指令を受信したか否かの判断がなされ、受信していない場合にはＳＣ４へ進み、ONモード指令を受信したか否かの判断がなされ、受信していない場合にはＳＣ３へ戻る。このＳＣ３→ＳＣ４→ＳＣ３のループの巡回途中で、ＳＢ４にしたがってブラウザフォン３０からOFFモード指令が発信されて来れば、ＳＣ３によりＹＥＳの判断がなされてＳＣ５へ進み、受信したパスワードを記憶する処理がなされ、ＳＣ６より、OFFモードに切換える処理がなされてＳＣ１へもどる。これにより、購入済み物品に付されているＲＦＩＤタグは、気億しているＲＦＩＤを発信しない発信停止状態に切換わる。

【０１０７】
一方、ＳＢ１０に従ってブラウザフォン３０からＯＮモード指令が発信されてくれば、ＳＣ４によりＹＥＳの判断がなされてＳＣ７へ進み、受信したパスワードと既に記憶しているパスワードとが一致しているか否かの判断を行なって本人認証を行なう処理がなされる。一致しない場合には、本人認証の確認ができないこととなり、ＳＣ１にもどるが、一致する場合には本人認証の確認ができたと判断してＳＣ８へ進み、ＯＮモードに切換える処理がなされる。これにより、購入済み物品に付されているＲＦＩＤタグは、記憶しているＲＦＩＤを発信可能な状態に切換わる。
【０１０８】
ＳＢ５またはＳＢ１１によりブラウザフォン３０からＲＦＩＤ発信指令があった場合あるいはタグリーダからＲＦＩＤ送信指令があった場合には、ＳＣ２によりＹＥＳの判断がなされてＳＣ９へ進み、ＯＮモード即ち記憶しているＲＦＩＤを発信可能なモードになっているか否かの判断がなされる。ＯＮモードになっていない場合にはＳＣ１へ戻るが、ＯＮモードになっている場合にはＳＣ１０へ進み、記憶しているＲＦＩＤを発信する処理がなされる。
【０１０９】
図１７は、図２に示したＶＰ管理サーバ９の処理動作を示すフローチャートである。ステップＳ１により、ＶＰの出生依頼があったか否かの判断がなされる。顧客（ユーザ）がブラウザフォン３０を操作してＶＰの出生依頼を行なえば、Ｓ１ａに進み、正当機関である旨の証明処理がなされる。この証明処理は、金融機関７がＶＰの管理をする正当な機関であることを証明するための処理であり、他人が金融機関７になりすます不正行為を防止するための処理である。この処理については、図２４（ｂ）に基づいて後述する。次にＳ２へ進み、ＲＰの氏名，住所の入力要求をブラウザフォン３０へ送信する。次にＳ３へ進み、ＲＰの氏名，住所の返信がブラウザフォン３０からあったか否かの判断がなされ、あるまで待機する。
【０１１０】
ユーザであるＲＰがブラウザフォン３０から自分の氏名，住所を入力して送信すれば、Ｓ３によりＹＥＳの判断がなされてＳ４へ進み、乱数Ｒを生成してチャレンジデータとしてブラウザフォン３０へ送信する処理がなされる。ユーザがＶＰの出生依頼を行なう場合には、ブラウザフォン３０のＵＳＢポート１８にＶＰ用ＩＣ端末１９Ｖを差込んでおく。その状態で、ＶＰ管理サーバ９から乱数Ｒが送信されてくれば、その乱数をＶＰ用ＩＣ端末１９Ｖへ入力する。すると、後述するように、ＶＰ用ＩＣ端末１９Ｖ内において入力された乱数ＲをＲＰの認証鍵ＫＮを用いて暗号化する処理がなされ、その暗号結果がブラウザフォン３０へ出力される。ブラウザフォン３０では、その出力されてきた暗号化データであるレスポンスデータＩをＶＰ管理サーバ９へ送信する。すると、Ｓ５によりＹＥＳの判断がなされてＳ６へ進み、ＲＰの認証鍵ＫＮを用いて、受信したレスポンスデータＩを復号化する処理すなわちD_{KN}（Ｉ）を算出する処理がなされる。次にＳ７へ進み、Ｓ４により生成した乱数Ｒ＝D_{KN}（Ｉ）であるか否かの判断がなされる。
【０１１１】
ＶＰの出生依頼者が金融機関７のデータベース１２に記憶されている正規のＲＰである場合には、Ｒ＝D_{KN}（Ｉ）となるために、制御がＳ９へ進むが、データベース１２に記憶されているＲＰに他人がなりすましてＶＰの出生依頼を行なった場合には、Ｒ＝D_{KN}（Ｉ）とはならないために、制御がＳ８へ進み、アクセス拒絶の旨がブラウザフォン３０へ送信されてＳ１へ戻る。
【０１１２】
一方、Ｓ７によりＹＥＳの判断がなされた場合には、Ｓ９へ進み、希望のコンビニエンスストアの入力があったか否かの判断がなされる。ＶＰの出生依頼を行なったＲＰは、誕生してくるＶＰの住所となるコンビニエンスストアについて特に希望するコンビニエンスストアがあれば、ブラウザフォン３０に入力してＶＰ管理サーバ９へ送信する。その場合には、Ｓ９によりＹＥＳの判断がなされてＳ１０へ進み、その入力されてきたコンビニエ

ンスストアの情報を記憶した後Ｓ１２へ進む。一方、希望するコンビニエンスストアの入力がなかった場合にはＳ１１へ進み、ＲＰの住所に近いコンビニエンスストアを検索してそのコンビニエンスストアを記憶した後Ｓ１２へ進む。

【０１１３】

Ｓ１２では、ＶＰの氏名，ＶＰの住所であるコンビニエンスストアの住所，ＶＰのＥメールアドレス等を決定する。次にＳ１３へ進み、ＶＰの公開鍵の送信要求をブラウザフォン３０へ送信する。そして、Ｓ１４へ進み、公開鍵ＫＰの返信があったか否かの判断がなされ、あるまで待機する。ＶＰの公開鍵の送信要求を受けたブラウザフォン３０は、接続されているＶＰ用ＩＣ端末１９Ｖへ公開鍵出力要求を出力する。すると、後述するように、ＶＰ用ＩＣ端末１９Ｖは、記憶しているＶＰ用の公開鍵ＫＰをブラウザフォン３０へ出力する。ブラウザフォン３０では、その出力されてきたＶＰ用の公開鍵ＫＰをＶＰ管理サーバ９へ返信する。すると、Ｓ１４よりＹＥＳの判断がなされてＳ１５へ進み、ＲＰに対応付けて、ＶＰの氏名，住所，公開鍵ＫＰ，Ｅメールアドレスをデータベース１２へ記憶させる処理がなされる。

【０１１４】

次にＳ１６へ進み、ＶＰの電子証明書を作成してＸＭＬストア５０に登録する処理がなされる。この電子証明書は、金融機関７等の第三者機関においてＲＰとの対応関係が登録されている正規のＶＰであることを証明するものである。次にＳ１７へ進み、ＲＰに、ＶＰの氏名，コンビニエンスストアの住所，コンビニエンスストアの名称，Ｅメールアドレス，電子証明書を記憶したＩＣ端末１９Ｉを郵送するための処理がなされる。次にＳ１８へ進み、Ｓ１２で決定された住所のコンビニエンスストアにＶＰの氏名，Ｅメールアドレス，当該金融機関７の名称を送信する処理がなされる。次にＳ１９へ進み、正当機関である旨の証明処理がなされる。この正当機関である旨の証明処理は、前述したＳ１ａと同じ処理である。次にＳ１へ戻る。

【０１１５】

本発明でいう「匿名用の電子証明書」とは、ユーザと当該ユーザが用いる匿名（ＶＰ氏名）との対応関係を特定可能な情報を登録している守秘義務のある所定機関（金融機関７）により発行され、前記匿名を用いるユーザが当該所定機関に登録されているユーザであることを証明する証明書を含む概念である。よって、本人確認に用いる一般的なデジタルＩＤばかりでなく、前記所定機関が前記匿名を用いるユーザに対し当該ユーザは当該所定機関に登録されているユーザであることを証明する電子的な証明書をすべて含む概念である。たとえば、ユーザが用いる匿名とその匿名が前記所定機関に登録されているメッセージとに対し、前記所定機関によるデジタル署名が施されただけの、簡単な証明書を含む概念である。

【０１１６】

Ｓ１によりＮＯの判断がなされた場合には図１８（ａ）のＳ４００へ進む。Ｓ４００では、個人情報の登録処理が行なわれ、次にＳ４０１によりトラップ情報の登録処理が行なわれ、Ｓ４０２により個人情報の確認処理が行なわれ、Ｓ４０３により個人情報の照合，流通チェック処理が行なわれ、Ｓ４０４により個人情報の販売代行処理が行なわれ、Ｓ４０５によりメール転送，流通チェック処理が行なわれてＳ１へ戻る。ユーザから個人情報の提供を受けたサイト（業者）側では、提供してもらった個人情報が本当に正しい内容であるか否かを確認したいというニーズがある。そこで、金融機関７のＶＰ管理サーバ９は、ユーザから個人情報を受付けてその個人情報が正しい個人情報かどうかをチェックし、正しい個人情報のみをデータベース１２ａに登録する。その処理をＳ４００により行なう。

【０１１７】

一方、ネットワーク上でＶＰの利用が盛んになった場合には、ＲＰとＶＰとの両方の詳しい個人情報を収集した業者が、両個人情報をしらみつぶしにマッチングして、両個人情報が一致するＲＰ氏名とＶＰ氏名とを割出し、ＶＰに対応するＲＰを予測してしまうという不都合が生ずる恐れがある。そこで、個人情報をデータベース１２ａに登録する場合に

は、勤務先名や所属部署名あるいは役職等のＲＰが特定されてしまうような個人情報を排除（または変更）して、登録する必要がある。そのような処理を、Ｓ４００により行なう。

【０１１８】

一方、個人情報主であるユーザは、自己の個人情報が正しい内容で流通しているか否かを監視し、間違っていれば正しい内容に修正したいというニーズがある。そこで、データベース１２ｂに登録されている自己の個人情報の真偽をユーザがチェックできるように、Ｓ４０２により、個人情報の確認処理が行なわれる。

【０１１９】

さらに、ユーザが自己の個人情報の公開範囲（流通範囲）を限定した上でその個人情報を業者側（サイト側）に提供した場合に、その公開範囲（流通範囲）が守られているか否かを監視したいというニーズがある。個人情報の提供を受けた業者側は、前述したようにその個人情報が正しい情報であるか否かを確認したいというニーズがある。そこで、サイト側（業者側）が所有している個人情報を正しい個人情報が登録されているデータベース１２ａの個人情報と照合できるようにする一方、その照合対象となった業者側所有の個人情報の流通許容範囲をチェックして正しく流通されているか否かをチェックできるように、Ｓ４０３の処理が行なわれる。

【０１２０】

ユーザは、個人情報を提供する見返りとして、何らかのサービスあるいは金銭を入手したいというニーズがある。そこで、Ｓ４０４により、個人情報の販売代行が行なわれる。図３に基づいて説明したように、トラップ型ＶＰは、Ｅメールアドレスを金融機関７のトラップ型ＶＰ用として開設しているアドレスにしているため、そのトラップ型ＶＰに宛てたＥメールは金融機関７のトラップ型ＶＰ用に開設されたＥメールアドレス宛に送られる。そこで、その送られてきたＥメールを対応するＶＰのＥメールアドレスに転送する必要がある。その処理を、Ｓ４０５により行なう。その際に、業者側から送られてくるＥメールの宛名はトラップ型ＶＰとなっているために、そのトラップ型ＶＰに対応するサイト（業社）を割出し（図３参照）、その割出されたサイト（業社）からのＥメールでなかった場合には当該トラップ型ＶＰの個人情報の流通許容範囲内のサイト（業社）からのＥメールか否かをチェックし、流通チェックを行なうことも、Ｓ４０５により行なわれる。

【０１２１】

図１８（ｂ）は、Ｓ４００の個人情報の登録処理のサブルーチンプログラムを示すフローチャートである。この個人情報の登録処理は、ユーザがＶＰとして個人情報を登録する際の処理である。

【０１２２】

乱数Ｒを受信したブラウザフォン３０は、そのブラウザフォン３０に接続されているＶＰ用ＩＣ端末１９Ｖに記憶されているＶＰ用の秘密鍵を用いて乱数Ｒを１回暗号化してレスポンスデータＩを生成する。そしてそのレスポンスデータＩを金融機関７のＶＰ用管理サーバ９へ送信する。

【０１２３】

Ｓ４１０により、ユーザ側から個人情報の登録要求があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。登録要求があった場合にはＳ４１１へ進み、正当機関証明処理がなされる。次に制御がＳ４１２へ進み、ＶＰの氏名の入力要求がなされ、Ｓ４１３により入力があったか否かの判断がなされる。入力があった場合には制御がＳ４１４へ進み、乱数Ｒを生成してチャレンジデータとして登録要求を行なったユーザ側に送信する処理がなされる。Ｓ４１５へ進み、ユーザ側からレスポンスデータＩを受信したか否かの判断がなされ、受信するまで待機する。受信した段階でＳ４１６へ進み、ＶＰの公開鍵ＫＰをデータベース１２ａから検索して、受信したレスポンスデータＩを公開鍵ＫＰで暗号化したD_{KP}（Ｉ）を生成する処理がなされる。

【０１２４】

次に制御がＳ４１７へ進み、チャレンジデータＲとD_{KP}（Ｉ）が等しいか否かの判断が

なされる。等しくなければユーザの本人認証ができなかったこととなりＳ４２２へ進み、登録拒否の処理がなされる。Ｓ４１７によりＹＥＳの判断がなされた場合には制御がＳ４１８へ進み、登録要求を出したユーザに対し登録を希望する個人情報の入力要求を出す処理がなされる。次にＳ４１９へ進み、入力があったか否かの判断がなされ、入力があるまで待機する。入力があった段階で制御がＳ４２０へ進み、登録対象の個人情報の真偽チェックを行なう。

【０１２５】

この真偽チェックは、たとえば、ＸＭＬストア５０にアクセスして該当するユーザの個人情報が登録されている場合にそれと照合チェックしたり、電子行政群４９に含まれる市役所等にアクセスしてそこに登録されている個人情報と照合チェックしたりして行なわれる。このような機械検索による照合チェックだけでは不十分な場合には、金融機関７の調査員が裏取り調査を行なって真偽チェックを行なう。

【０１２６】

次に制御がＳ４２１へ進み、真偽チェックの結果正しいか否かの判断がなされ、正しくない場合にはＳ４２２へ進み登録拒否の処理がなされる一方、正しい場合にはＳ４２３へ進み、ＲＰが特定される個人情報か否かの判断がなされる。登録しようとしているＶＰの個人情報の中に、たとえば勤務先名や所属部署名あるいは役職等のＲＰが特定されてしまうような個人情報が存在する場合に、それをそのまま登録してしまうと、その登録情報からどのＶＰがどのＲＰに対応するかを第三者に予測されてしまう恐れがある。このデータベース１２ａに登録される個人情報は、Ｓ４０３やＳ４０４によりサイト側（業者側）が知り得る状態となる。その結果、サイト側（業者側）に、ＲＰとＶＰとの対応関係が予測される恐れが生ずる。

【０１２７】

そこで、Ｓ４２３により、ＲＰが特定される個人情報か否かの判断がなされ、予測される個人情報でなければＳ４２５へ進むが、予測される恐れのある個人情報の場合にはＳ４２４へ進み、その個人情報を加工する処理がなされた後Ｓ４２５へ進む。たとえば、勤務先名がＭＥＣであった場合には、それをたとえば「某大手電気メーカー」に加工したり、役職がたとえば専務であった場合には、たとえば「重役」に加工したりする。

【０１２８】

Ｓ４２５では、個人情報に当該金融機関のデジタル署名を付してユーザ名別に登録する処理がなされる。その結果、図４に示すようなデータがデータベース１２ａに登録される。

【０１２９】

図１９は、Ｓ４０１に示されたトラップ情報の登録処理のサブルーチンプログラムを示すフローチャートである。Ｓ４３０により、正当機関証明処理がなされ、Ｓ４３１により、ＶＰ氏名の入力要求がトラップ情報の登録依頼をしてきたＶＰに出される。次にＳ４３２へ進み、その登録依頼をしてきたＶＰが自己のＶＰ氏名を入力したか否かの判断がなされ、入力するまでＳ４３１の要求が出される。次に制御がＳ４３３へ進み、乱数Ｒを生成してチャレンジデータとして登録依頼者であるＶＰに送信する処理がなされる。Ｓ４３４により、レスポンスデータＩを受信したか否かの判断がなされる。

【０１３０】

送信されてきたチャレンジデータＲを受信した登録依頼者であるＶＰがそのチャレンジデータＲを自己の秘密鍵で暗号化してレスポンスデータＩを生成し、金融機関７のＶＰ管理サーバ９へ送信する。すると、制御がＳ４３５へ進み、登録依頼をしてきたＶＰの公開鍵ＫＰをデータベース１２ａから検索し、受信したレスポンスデータＩをその公開鍵ＫＰで復号化する処理を行なう。そしてＳ４３６により、チャレンジデータ$R=D_{KP}(I)$であるか否かの判断がなされ、イコールでない場合には認証の結果そのＶＰが本人と確定できないということであり、Ｓ４３７により登録拒否の通知がそのＶＰになされる。一方、Ｓ４３６によりＹＥＳの判断がなされて認証の結果ＶＰが本人であることが確認できた場合には、制御がＳ４３８へ進み、トラップ情報の送信要求をそのＶＰへ送信する処理がな

される。

【０１３１】

ＶＰから登録してもらいたいトラップ情報が送信されてきたか否かがＳ４３９によりなされ、送信されてくるまで待機する。送信されてきた段階で制御がＳ４４０へ進み、送信されてきたトラップ情報をデータベース１２ａに記憶させる処理がなされる。このトラップ情報は、登録依頼者であるＶＰに対応した記憶領域に記憶される。次に制御がＳ４４１へ進み、そのトラップ情報に対する電子署名を金融機関７が生成して、その電子証明書をＸＭＬストア５０へ登録する処理がなされる。その結果、図５に基づいて説明したように、ＸＭＬストア５０のデータベース７２に電子証明書が格納される。

【０１３２】

この電子証明書は、ＸＭＬストア５０に格納する代わりに登録依頼を行なってきたＶＰのＩＣ端末１９Ｖに格納してもよい。しかし、トラップ情報は、前述したように、そのＶＰがアクセスしたＷｅｂサイト毎またはＶＰ（トラップ型ＶＰ）として登録してポイントカードを新規発行してもらった百貨店等の業社毎に異なり、その結果電子証明書もＷｅｂサイト毎（業社毎）に異なることとなり、多数の電子証明書をＩＣ端末１９Ｖに格納するとなると、記憶容量の問題が生ずる。ゆえに、本実施の形態では、その記憶容量の問題を克服するために、ＸＭＬストア５０へ登録する。なお、ＩＣ端末１９Ｖの記憶容量が非常に大きなものであれば、金融機関７が発行した電子証明書のすべてまたはその大半をこのＩＣ端末１９Ｖに記憶させてもよい。

【０１３３】

図２０は、Ｓ４０５に示されたメール転送，流通チェックのサブルーチンプログラムを示すフローチャートである。Ｓ５１４により、サイト（業者）からメールが送られてきたか否かの判断がなされる。図３等に基づいて説明したように、ＶＰが、本名を用いてサイトにアクセスしたり業社にポイントカードを登録した場合にはＶＰ自身のＥメールアドレスをそのサイト側（業社側）に通知するが、トラップ型ＶＰ氏名を用いてサイト（業社）にアクセスした場合には、金融機関７のトラップ型ＶＰ用として開設されているＥメールアドレスをそのサイト（業社）側に提供する。その結果、そのサイト（業社）からのＥメールは、金融機関７のトラップ型ＶＰ用に開設されたＥメールアドレスで送られてくることとなる。

【０１３４】

金融機関７では、そのトラップ型ＶＰ用に開設したＥメールアドレスに送信されてきたメールがある場合には、ＶＰ管理用サーバ９は、Ｓ５１４により、ＹＥＳの判断を行なう。その結果、制御がＳ５１５へ進み、その送られてきたＥメールに含まれている宛名に対応するサイト名（業者名）をデータベース１２ａから割出す処理を行なう。データベース１２ａは、図３に基づいて説明したように、ＶＰの氏名とそのＶＰがアクセスしたサイト名（業社名）とが対応付けられて記憶されている。この対応関係を利用して、メールの宛名から対応するサイト名（業者名）を割出す処理がなされる。

【０１３５】

次にＳ５１６により、割出されたサイト名（業社名）とＥメールを送ったサイト名（業社名）とが一致するか否かの判断がなされる。本来なら一致する筈であるが、個人情報が不正に流通された場合には、その不正流通された個人情報を不正入手したサイト（業社）がその個人情報主にＥメールを送る場合がある。その場合には、割出されたサイト名（業社名）とメールを送ったサイト名（業社名）とが一致しない状態となる。

【０１３６】

割出されたサイト名（業社名）とメールを送ったサイト名（業社名）とが一致しない場合に、即座に個人情報が不正流通されたとは断定できない。サイト（業社）側に個人情報を提供する際に、ある一定の流通許容範囲内においては流通させてもよいと個人情報主であるユーザから承諾を得ている場合がある。よって、Ｓ５２２に制御が進み、ＸＭＬストアの該当個人情報を検索して、ポリシーに定められている流通許容範囲内にＥメール送信者が含まれるか否かチェックする処理がなされ、Ｓ５２３により、含まれると判断された

場合には制御がＳ５１７へ進むが、含まれないと判断された場合には制御がＳ５１９へ進む。

【０１３７】

Ｓ５１９では、Ｅメールを送ったサイト名（業社名）に対応させて個人情報の不正入手値を「１」加算更新する処理がなされ、Ｓ５２０により、Ｓ５１５によって割出されたサイト名（業社名）に対応させて個人情報の不正流出値を「１」加算更新する処理がなされる。次にＳ５２１により、個人情報の不正があった旨およびその詳細データを該当するユーザへ通知する処理がなされる。

【０１３８】

一方、個人情報が不正流通されていないと判断された場合には制御がＳ５１７へ進み、Ｅメールの宛名に対応するユーザのメールアドレスを割出す処理がなされ、Ｓ５１８により、その割出されたアドレスにＥメールを転送する処理がなされる。

【０１３９】

図２１は、図２に示した認証用サーバ１１の処理動作を示すフローチャートである。先ずＳ２５により、ＲＰから電子証明書の発行依頼があったか否かの判断がなされ、あるまで待機する。ユーザであるＲＰがブラウザフォン３０からＲＰの電子証明書の発行依頼要求を認証用サーバ１１へ送信すれば、制御がＳ２６へ進み、ＲＰの住所，氏名，公開鍵の送信要求をブラウザフォン３０へ送信する処理がなされる。次にＳ２７へ進み、ブラウザフォン３０からＲＰの住所，氏名，公開鍵の返信があるか否かの判断がなされ、あるまで待機する。そして、返信があった段階で制御がＳ２８へ進み、ＲＰの電子証明書を作成してブラウザフォン３０へ送信する処理がなされる。次にＳ２９へ進み、ＲＰの住所，氏名，公開鍵ＫＰをデータベース１２ａに記憶する処理がなされてＳ２５へ戻る。

【０１４０】

図２２～図２４は、図２の決済サーバ１０の処理動作を示すフローチャートである。Ｓ３５により、ＲＰの銀行口座番号の作成依頼があったか否かの判断がなされ、ない場合にはＳ３９へ進み、ＶＰの銀行口座番号の作成依頼があったか否かの判断がなされ、ない場合にはＳ４０へ進み、デビットカードの発行要求があったか否かの判断がなされ、ない場合にはＳ４１へ進み、決済要求があったか否かの判断がなされ、ない場合にはＳ３５へ戻る。

【０１４１】

このＳ３５～Ｓ４１のループの巡回途中で、ユーザが金融機関７へ出向き、ＲＰの銀行口座の開設依頼を行なってＲＰの銀行口座番号の作成依頼が入力されれば、制御がＳ３６へ進み、ＲＰの住所，氏名等の入力要求がなされ、入力があれば制御がＳ３８へ進み、ＲＰの銀行口座を作成して、データベース１２ａに記憶するとともにＲＰに通知する処理がなされてＳ３５へ戻る。

【０１４２】

ユーザが金融機関７へ出向き、ＶＰの銀行口座の開設依頼を行なってＶＰの銀行口座番号の作成依頼要求が入力されれば、Ｓ４２へ進み、ＶＰの住所，氏名等，ＲＰの住所，氏名等の入力要求がなされる。ユーザは、これら情報を手動でキーボードから入力するか、または、決済サーバ１０にＲＰ用ＩＣ端末１９ＲやＶＰ用ＩＣ端末１９Ｖを接続してこれらデータを自動入力する。データが入力されれば、制御がＳ４４へ進み、ＲＰとＶＰの対応が適正であるか否かが、データベース１２ａを検索することにより確認される。

【０１４３】

ＲＰとＶＰの対応が適正でない場合にはＳ５１へ進み、対応が不適正である旨を報知してＳ３５へ戻る。一方、ＲＰとＶＰとの対応が適正な場合にはＳ４５へ進み、ＶＰの銀行口座を作成して、データベース１２ａに記憶するとともに、ＶＰに対応するＲＰにその銀行口座を郵送する処理がなされた後Ｓ３５へ戻る。

【０１４４】

ユーザが金融機関７へ出向き、デビットカードの発行要求の依頼を行なってデビットカードの発行要求の入力があれば、Ｓ４０によりＹＥＳの判断がなされてＳ４６へ進み、口

座番号と氏名と暗証番号の入力要求がなされる。ユーザがＲＰ用のデビットカードの発行を要求する場合には、ＲＰの銀行口座番号と氏名と暗証番号を入力する。一方、ユーザがＶＰ用のデビットカードの発行要求を希望する場合には、ＶＰの銀行口座番号とＶＰの氏名とＶＰの暗証番号とを入力する。これらのデータの入力は、ＲＰ用ＩＣ端末１９ＲまたはＶＰ用ＩＣ端末１９Ｖを決済サーバ１０へ接続して自動的に入力する。

【０１４５】

これらデータの入力が行なわれれば制御がＳ４８へ進み、入力データをデータベース１２ａへ記憶するとともに、デビットカードを発行する処理がなされる。次にＳ４９へ進み、発行されたデビットカードの記憶データをＲＰ用ＩＣ端末またはＶＰ用ＩＣ端末へ伝送する処理がなされてＳ３５へ戻る。

【０１４６】

決済サーバ１０に決済要求が送信されてくれば、Ｓ４１によりＹＥＳの判断がなされてＳ５０へ進み、決済処理がなされた後Ｓ３５へ戻る。

【０１４７】

図２３は、図２２に示したＳ５０の決済処理のサブルーチンプログラムを示すフローチャートである。決済要求には、銀行口座内の資金を一部ＲＰ用ＩＣ端末１９ＲまたはＶＰ用ＩＣ端末１９Ｖに引落す引落し要求と、デビットカードを使用しての決済要求と、クレジットカードを使用して決済を行なった場合のクレジットカード発行会社からのクレジット使用金額の引落し要求とがある。まずＳ５５よりＩＣ端末１９Ｒまたは１９Ｖへの引落し要求があったか否かの判断がなされ、ない場合にはＳ５７へ進み、デビットカードを使用しての決済要求があったか否かの判断がなされ、ない場合にはＳ５８へ進み、クレジットカード発行会社からの引落し要求があったか否かの判断がなされ、ない場合にはＳ５５４へ進み、クレジットカード発行会社からの問合せ処理が行なわれた後、Ｓ５９によりその他の処理がなされてこのサブルーチンプログラムが終了する。

【０１４８】

ユーザがブラウザフォン３０等からＲＰ用ＩＣ端末１９ＲまたはＶＰ用ＩＣ端末１９Ｖへ資金の一部引落し要求を決済サーバ１０へ送信した場合には、Ｓ５５によりＹＥＳの判断がなされてＳ５６へ進み、正当機関証明処理がなされた後Ｓ６０へ進む。Ｓ６０では、氏名の入力要求をブラウザフォン３０等へ送信する処理がなされる。その要求を受けたブラウザフォン３０では、接続されているＩＣ端末１９Ｒまたは１９Ｖに対し氏名の出力要求を伝送する。すると、接続されているＩＣ端末１９Ｒまたは１９Ｖから氏名がブラウザフォン３０へ伝送され、その伝送されてきた氏名をブラウザフォン３０が決済サーバ１０へ伝送する。すると、Ｓ６１によりＹＥＳの判断がなされてＳ６２へ進み、乱数Ｒを生成してチャレンジデータとしてブラウザフォン３０へ送信する処理がなされる。

【０１４９】

その乱数Ｒを受けたブラウザフォン３０は、後述するように、接続されているＩＣ端末１９Ｒまたは１９Ｖに対し乱数Ｒを伝送する。乱数Ｒを受取ったＩＣ端末がＲＰ用ＩＣ端末１９Ｒの場合には、記憶している認証鍵ＫＮを用いてＲを暗号化してレスポンスデータＩを生成し、それをブラウザフォン３０へ出力する。ブラウザフォン３０では、その出力されてきたレスポンスデータＩを決済サーバ１０へ送信する。一方、乱数Ｒを受取ったＩＣ端末がＶＰ用ＩＣ端末１９Ｖの場合には、受取った乱数Ｒを記憶している公開鍵ＫＰを用いて暗号化してレスポンスデータＩを生成し、ブラウザフォン３０へ出力する。ブラウザフォン３０では、その出力されてきたレスポンスデータＩを決済サーバ１０へ送信する。

【０１５０】

レスポンスデータＩが送信されてくれば、Ｓ６３によりＹＥＳの判断がなされてＳ６４に進み、Ｓ６０に応じて入力された氏名がＲＰのものであるか否かが判別され、ＲＰの場合にはＳ６５へ進み、ＲＰの認証鍵ＫＮをデータベース１２から検索してその認証鍵ＫＮを用いて受信したレスポンスデータＩを復号化する処理すなわちD_{KN}（Ｉ）を生成する処理がなされる。次にＳ６６へ進み、Ｒ＝D_{KN}（Ｉ）であるか否かの判断がなされる。ＩＣ

端末への引落し要求を行なったユーザがデータベース１２に登録されている適正なユーザである場合には、Ｒ＝D_{NK}（Ｉ）となるはずであるが、データベース１２に登録されているユーザになりすまして銀行口座の資金の一部を引落しするという不正行為が行われた場合には、ＲとD_{KN}（Ｉ）とが一致しない状態となる。その場合には制御がＳ７９へ進み、不適正である旨をブラウザフォン３０へ返信する処理がなされてサブルーチンプログラムが終了する。

【０１５１】

一方、Ｒ＝D_{KN}（Ｉ）の場合には制御がＳ６７へ進み、引落し額の入力要求をブラウザフォン３０へ送信する処理がなされ、引落し額がブラウザフォン３０から送信されてくれば、制御がＳ６９へ進み、ＲＰの口座から引落し額Ｇを減算してＧをブラウザフォン３０へ送信する処理がなされてサブルーチンプログラムが終了する。

【０１５２】

一方、ユーザがＶＰとしてＶＰ用ＩＣ端末１９Ｖへの引落しを行なう場合には、ＶＰの本名を用いる。入力された氏名がＶＰの本名であった場合にはＳ６４によりＮＯの判断がなされて制御が図２４（ａ）のＳ８５へ進む。Ｓ８５では、ＶＰの公開鍵ＫＰをデータベース１２から検索してその公開鍵ＫＰを用いて受信したレスポンスデータＩを復号化する処理すなわちD_{KP}（Ｉ）を生成する処理がなされる。次にＳ８６へ進み、Ｒ＝D_{KP}（Ｉ）であるか否かの判断がなされる。引落し要求を行なっているものがデータベース１２に登録されているＶＰになりすまして引落すという不正行為を行なっている場合には、Ｓ８６によりＮＯの判断がなされてＳ７９に進み、不適正である旨がブラウザフォン３０へ返信されることとなる。一方、Ｓ８６によりＹＥＳの判断がなされた場合にはＳ８７へ進み、引落し額Ｇの入力要求をブラウザフォン３０へ送信する処理がなされ、ブラウザフォン３０から引落し額Ｇの送信があれば、Ｓ８９へ進み、ＶＰの銀行口座からＧを減算してＧをブラウザフォン３０へ送信する処理がなされた後サブルーチンプログラムが終了する。

【０１５３】

ユーザがデビットカードを使用しての決済を行なうべくデビットカード使用操作を行なった場合には、デビットカード使用要求が決済サーバ１０へ送信され、Ｓ５７によりＹＥＳの判断がなされてＳ５６へ進み、正当機関証明処理がなされる。次にＳ７０へ進み、暗証番号とカード情報入力要求がユーザのブラウザフォン３０へ送信される。デビットカードの暗証番号とデビットカード情報とがブラウザフォン３０から決済サーバ１０へ送信されてくれば制御がＳ７２へ進み、その送信されてきたデータが適正であるか否かの判断がなされ、不適正であればＳ７９へ進む。

【０１５４】

一方、適正である場合にはＳ７３へ進み、使用額Ｇの入力を待つ。ユーザが使用額Ｇを入力してそれが決済サーバ１０へ送信されてくれば制御がＳ７４へ進み、該当する口座を検索してＧを減算するとともにＧをユーザのブラウザフォン３０に送信する処理がなされる。

【０１５５】

ユーザがＲＰまたはＶＰの本名を用いて後述するようにクレジットカードによるＳＥＴを用いた決済を行なった場合には、クレジットカード発行会社４（図１参照）からクレジット支払金額の引落し要求が決済サーバ１０へ送信される。その引落し要求が送信されてくればＳ５８によりＹＥＳの判断がなされてＳ５６の正当機関証明処理がなされた後Ｓ７５へ進み、ユーザの氏名，口座番号の入力を待つ。クレジットカード発行会社４からユーザの氏名と口座番号とが送信されてくれば制御がＳ７６へ進み、その入力されたデータが適正であるか否かをデータベース１２を検索して判別する。不適正の場合にはＳ７９へ進むが、適正な場合にはＳ７７へ進み、引落し額Ｇの入力を待機する。クレジットカード発行会社４から引落し額Ｇすなわちクレジット支払額と手数料との合計金額が送信されてくれば制御がＳ７８へ進み、口座からＧを減算してクレジットカード発行会社の口座Ｇに加算する処理すなわち資金の移動処理がなされる。

【０１５６】

Ｓ５８によりＮＯの判断がなされた場合にはＳ５５４によるクレジット発行会社４からの問合せ処理が行なわれた後Ｓ５９へ進み、その他の処理が行なわれる。

【０１５７】

図２４（ｂ）は、前述したＳ１ａ，Ｓ１９，Ｓ５６に示された正当機関証明処理のサブルーチンプログラムを示すフローチャートである。まずＳ９０により、当該機関の電子証明書を送信する処理がなされる。この電子証明書を受信した側においては、乱数Ｒを生成してその乱数Ｒを送信する。すると、Ｓ９１によりＹＥＳの判断がなされてＳ９２へ進み、その受信した乱数Ｒを当該機関の秘密鍵ＫＳで暗号化する処理すなわちＬ＝E_{KS}（Ｒ）を算出する処理がなされ、その算出されたＬを返信する処理がなされる。

【０１５８】

このＬを受信した受信側においては、既に受信している電子証明書内の当該機関の公開鍵ＫＰを利用してＬを復号化することによりＲを得ることができる。そのＲと送信したＲとがイコールであるか否かをチェックすることにより、正当機関であるか否かをチェックすることが可能となる。これについては後述する。

【０１５９】

図２５は、Ｓ５５４に示されたクレジットカード会社からの問合せ処理のサブルーチンプログラムを示すフローチャートである。前述したように、ＶＰがトラップ型ＶＰとしてサイトにアクセスして電子ショッピング等を行なったりトラップ型ＶＰとして登録している小売店等の業社で自動決済を行ってクレジット決済を行なった場合には、ＶＰ本人のクレジット番号が用いられるのではなく、そのＶＰ本人のクレジット番号を何回か秘密鍵で暗号化した暗号化クレジット番号が用いられることとなる。たとえば、図３に示すように、トラップ型ＶＰ氏名Ｅ（Ｂ１３Ｐ）としてサイトＭＰＰにアクセスしたＶＰは、電子ショッピング等を行なってクレジット決済をする際には、バーチャルクレジット番号Ｅ（３２８８）を用いる。ＶＰは、クレジットカード発行会社４に対し３２８８のクレジット番号は登録しているが、Ｅ（３２８８）の暗号化クレジット番号までは登録していない。よって、Ｅ（３２８８）のバーチャルクレジット番号がクレジット決済に伴ってクレジットカード発行会社４に送信されてきた場合には、クレジットカード発行会社４は、そのＥ（３２８８）のバーチャルクレジット番号を自社で検索して真偽を確かめることはできない。

【０１６０】

そこで、そのような場合に、クレジットカード発行会社は、金融機関７にそのバーチャルクレジット番号が正しいか否かの照会を行なってもらうのである。

【０１６１】

クレジットカード発行会社からの問合せがあれば制御はＳ５６１へ進み、Ｓ５６１～Ｓ５６８の前述したものと同様の認証処理が行なわれる。認証の結果本人が確認されればＳ５６７によりＹＥＳの判断がなされてＳ５６９へ進み、照会対象データの入力要求がクレジットカード発行会社に送信される。この照会対象データとは、前述したバーチャルクレジット番号とトラップ型ＶＰ氏名とを含む。このトラップ型ＶＰ氏名をも入力されることにより、そのトラップ型ＶＰ氏名とバーチャルクレジット番号とが対応しているか否か等も照会できる。

【０１６２】

照会対象データがクレジットカード発行会社から送信されてくれば制御はＳ５７１へ進み、データベース１２ａを検索してその送信されてきた照会対象データと照合する処理がなされる。次にＳ５７２により、照合結果送られてきた照会対象データが適正であるか否かの判断がなされ、適正な場合にＳ５７３により、適正な旨をクレジットカード発行会社へ返信し、照合結果適正でない場合にはＳ５７４により、不適正な旨がクレジットカード発行会社に返信される。Ｓ５７３による適正な旨を返信する際には、Ｓ５７０により入力された照会対象データに対し適正な旨を表わす金融機関７側のデジタル署名を付し、そのデジタル署名付きデータが問合せをしたクレジットカード発行会社４へ返信されることとなる。

【０１６３】
図２６は、図１４のＳ９５ｂに示されたブラウザフォン３０の偽モード処理のサブルーチンプログラムを示すフローチャートである。ＳＤ１により、電源投入時であるか否かの判断がなされ、電源投入時でない場合にはＳＤ２に進み、偽モード操作があったか否かの判断がなされ、ない場合にはＳＤ３へ進み、偽モード解除操作があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。
【０１６４】
ブラウザフォン３０の電源が投入されればＳＤ１によりＹＥＳの判断がなされてＳＤ４へ進み、現在のモードの種類をブラウザフォン３０により表示する処理がなされる。ブラウザフォン３０のモードは、偽モード、トラップモード、通常モードの３種類があり、現在どのモードになっているかが、ＳＤ４により表示される。次に制御がＳＤ５へ進み、現在偽モードになっているか否かの判断がなされ、偽モードになっていない場合にはこの偽モード処理のサブルーチンプログラムが終了する。
【０１６５】
一方、偽モードになっている場合にはＳＤ６へ進み、本人認証のためのパスワードを発信させて個人ユーザが所持している購入済物品に付されているＲＦＩＤタグに記憶させる処理がなされる。次にＲＦＩＤにＯＦＦモード指令を発信する処理がＳＤ７により行なわれる。これにより、購入済物品に付されているＲＦＩＤタグが、前述したようにＯＦＦモード即ち記憶しているＲＦＩＤを発信しない発信停止モードとなる（ＳＣ６参照）。次にＳＤ８へ進み、購入済物品に付されているＲＦＩＤタグに対しＲＦＩＤ送信指令を発信し、ＳＤ９により、そのＲＦＩＤタグからＲＦＩＤが発信されてそれを受信したか否かの判断がなされる。通常であれば、発信停止モードに切換わった後であるためにＲＦＩＤは発信されてくることがなく、ＳＤ１０へ進み、ＲＦＩＤ交換処理がなされる。一方、ＳＤ９によりＲＦＩＤを受信した旨の判断がなされた場合には、ＳＤ１１へ進み、ブラウザフォン３０によりエラー表示がなされる。
【０１６６】
個人ユーザがブラウザフォン３０により偽モード操作を行なった場合には、ＳＤ２によりＹＥＳの判断がなされてＳＤ１２へ進み、ブラウザフォン３０を偽モードに切換える処理がなされた後にＳＤ６へ進む。一方、ブラウザフォン３０により偽モード解除操作が行われた場合には、ＳＤ３によりＹＥＳの判断がなされて、ＳＤ１３へ進み、ブラウザフォン３０の偽モードを解除して通常モードにする処理がなされる。
【０１６７】
尚、この偽ＲＦＩＤ発信機能を有するブラウザフォン３０を有する個人ユーザは、前述のセキュリティ用のＲＦＩＤタグ１ａを必ずしも所持する必要はない。ブラウザフォン３０がセキュリティ用のＲＦＩＤタグ１ａの代わりをしてくれるためである。
【０１６８】
図２７は、ＳＤ１０に示されたＲＦＩＤ交換処理のサブルーチンプログラムを示すフローチャートである。ＳＥ１により、交換希望電波をブラウザフォンから発信する処理がなされる。この交換希望電波は、最大２０メートルの範囲までしか到達しない電波である。尚、この交換希望電波の到達距離を手動操作により変更設定地点例えば2メートル或いは５メートル等のように変更できるように構成してもよい。次にＳＥ２に進み、交換エリア内即ち交換希望電波が到達する圏内から交換希望電波を受信したか否かの判断がなされる。受信した場合には、ＳＥ３へ進み、今日既に交換済みの相手（ブラウザフォン３０）であるか否かの判断がなされ、既に交換済みのブラウザフォン３０の場合には、交換処理を行なうことなくこのサブルーチンプログラムが終了する。交換済みの相手（ブラウザフォン３０）であるか否かの判断を可能にするべく、前述の交換希望電波とともにブラウザフォン３０を特定するためのＩＤコード等を送信してもよい。
【０１６９】
一方、今日まだＲＦＩＤの交換を行なっていない相手（ブラウザフォン３０）の場合には制御がＳＥ４へ進み、偽ＲＦＩＤを記憶しているか否かの判断がなされる。ブラウザフ

ォン３０のＥＥＰＲＯＭ１９４に偽ＲＦＩＤを記憶しておれば、制御がＳＥ８へ進み、その記憶している偽ＲＦＩＤ（たとえば記憶中の１番新しい偽ＲＦＩＤ）を交換相手のブラウザフォン３０に発信すると共に、相手のブラウザフォン３０から偽ＲＦＩＤを受信する処理がなされる。次にＳＥ９へ進み、ＥＥＰＲＯＭ１９４に既に記憶している偽ＲＦＩＤを１つずつ古い記憶エリア側にシフトし、記憶上限を超えた１番古い偽ＲＦＩＤを消去する処理がなされる。次にＳＥ１０へ進み、１番新しい記憶エリアに受信した偽ＲＦＩＤを記憶する処理がなされる。

【０１７０】

一方、ＥＥＰＲＯＭ１９４に偽ＲＦＩＤを全く記憶していない場合には制御がＳＥ５へ進み、個数決定用乱数ＫＲを生成して偽ＲＦＩＤの送信個数を決定する処理がなされる。次にＳＥ６へ進み、その決定された個数だけのＲＦＩＤのコードを決定するための乱数ＩＤＲを生成して偽ＲＦＩＤのコードを決定して発信する処理がなされる。次にＳＥ７へ進み、相手からの偽ＲＦＩＤを受信して１番新しい記憶エリアに記憶する処理がなされる。

【０１７１】

このＲＦＩＤ交換処理により、ブラウザフォン３０を所持している個人ユーザが例えばすれ違う時に記憶している互いの偽ＲＦＩＤが交換されて記憶されることとなる。その結果、比較的同じ場所を移動する個人ユーザ同士で偽ＲＦＩＤを交換しあって互いの共通偽ＲＦＩＤとして記憶して、ＲＦＩＤ送信要求があった場合にはその共通偽ＲＦＩＤを発信することができる状態となり、比較的同じ場所を移動する個人ユーザ同士で前述の異人物同一識別子発信現象を生じさせることができ、悪意のプライバシー侵害者を有効に撹乱することができる。

【０１７２】

図２８は、図１４のＳ９５ｃに示されたトラップモードを処理のサブルーチンプログラムを示すフローチャートである。ＳＦ１により、トラップモード操作があったか否かの判断がなされ、ない場合にはＳＦ２へ進み、トラップモード解除操作があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。個人ユーザが自己のブラウザフォン３０を操作してトラップモード操作を行なった場合には、ＳＦ１によりＹＥＳの判断がなされてＳＦ３進み、ブラウザフォン３０はトラップモードに切換わる。

【０１７３】

次にＳＦ４へ進み、当該ユーザが所持している購入済物品に付されているＲＦＩＤに対しパスワードを発信する処理がなされる。次にＳＦ５へ進み、ＯＦＦモード指令がそのＲＦＩＤへ発信される。次にＳＦ６により、ＲＦＩＤ送信指令が発信され、ＳＡＦ７により、ＲＦＩＤの受信があったか否かの判断がなされる。ＳＦ５により既にＯＦＦモード指令が発信されているために、当該ユーザが所持する購入済物品に付されているＲＦＩＤタグからＲＦＩＤが発信されることは通常あり得ない。よって、通常は、ＳＦ７によりＮＯの判断がなされて、制御がＳＦ７ａに進む。ＳＦ７ａでは、業社選択指定操作があるか否かの判断がなされる。ない場合にはＳＦ８へ進が、個人ユーザが自己のブラウザフォン３０により罠を仕掛ける相手業社を選択指定した場合には、制御がＳＦ７ｂに進み、選択指定された業者を記憶する処理がなされた後にＳＦ８へ進む。

【０１７４】

次に、ＳＦ８により、トラップモード切換え完了の表示がブラウザフォン３０によりなされる。一方、ＳＦ７によりＲＦＩＤの受信があったと判断された場合にはＳＦ９へ進み、ブラウザフォン３０によりエラー表示がなされる。

【０１７５】

次に、個人ユーザが自己のブラウザフォン３０を操作してトラップモード解除操作を行なった場合には、ＳＦ２によりＹＥＳの判断がなされてＳＦ１０へ進み、当該ブラウザフォン３０のトラップモードが解除される。

【０１７６】

図２９は、図１４のＳ９５ｄに示されたＲＦＩＤ発信処理のサブルーチンプログラムを示すフローチャートである。ＳＧ１により、ＲＦＩＤ送信指令を受信したか否かの判断が

なされる。受信していなければこのサブルーチンプログラムが終了する。一方、タグリーダからＲＦＩＤ送信指令が発信されれば、ブラウザフォン３０がそれを受信してＳＧ１によりＹＥＳの判断がなされ、ＳＧ２により、受信した旨の報知がブラウザフォン３０によりなされる。この報知は、具体的には、ブラウザフォン３０から受信音を発生させると共にＲＦＩＤ送信要求の電波を受信した旨の表示を液晶表示画面に示す。

【０１７７】

次に制御がＳＧ３へ進み、偽モードになっているか否かの判断がなされる。偽モードになっていない場合にはＳＧ４へ進み、トラップモードになっているか否かの判断がなされる。トラップモードになっていない場合即ち通常モードの場合にはこのサブルーチンプログラムが終了する。従って、通常モードの場合には、ＲＦＩＤ送信指令を受信したとしても、何らＲＦＩＤを発信する処理が行なわれない。

【０１７８】

ブラウザフォン３０は偽モードになっている場合にはＳＧ３によりＹＥＳの判断がなされて制御がＳＧ３ａへ進み、前回のＲＦＩＤの発信から５秒経過しているか否かの判断がなされる。５秒経過していない場合にはＳＧ３ｂへ進み、前回発信したＲＦＩＤと同じコードのＲＦＩＤを発信する処理がなされる。これは、タグリーダの読取り信頼性を向上させるべくタグリーダから短期間の間に連続して複数回ＲＦＩＤ送信要求が送られてくることを想定したものであり、その場合毎回ランダムに生成された偽ＲＦＩＤを発信したのでは、適正なＲＦＩＤとして読取ってくれない不都合が生じる。そこで、前回のＲＦＩＤ発信から５秒経過していない時には、前回と同じコードのＲＦＩＤを発信するようにし、偽ＲＦＩＤであることが見破られる不都合を防止できるようにしている。また、タグリーダの読取り信頼性を向上させる目的ではなく、受信したＲＦＩＤが本物のＲＦＩＤであるかまたは偽物のＲＦＩＤであるかを見極めるために連続して複数回ＲＦＩＤ送信要求を発信するタグリーダが設置される可能性も予測される。そのようなタイプのタグリーダが設置されたとしても、所定期間内（例えば５秒間）の範囲内で再度ＲＦＩＤ発信要求が行われてくれば、前回と同じコードのＲＦＩＤを送り返すために、偽ＲＦＩＤであることが見破られる不都合を防止できる。この場合、第１回目の偽ＲＦＩＤを送信した後一旦電源用電波が停止され、その後（例えば５秒後）再度電源用電波が発信されてＲＦＩＤ発信要求が行われたとしても、コンデンサ１１０からの供給電力によりＲＦＩＤタグ１ａが作動中であるため、前回と同じ偽ＲＦＩＤを再発信することができる。

【０１７９】

前回のＲＦＩＤの発信から５秒経過している場合にはＳＧ３ａによりＹＥＳの判断がなされてＳＧ５へ進み、偽ＲＦＩＤがＥＥＰＲＯＭ１９４に記憶されているか否かの判断がなされる。記憶されている場合には、ＳＧ９へ進み、その記憶している偽ＲＦＩＤの内前回発信したＲＦＩＤの次の順番のＲＦＩＤを発信する処理がなされる。一方、偽ＲＦＩＤの記憶がない場合には、ＳＧ６へ進み、個数決定用乱数ＫＲを生成してＲＦＩＤの送信個数を決定する処理がなされ、ＳＧ７により、その決定された個数だけのＲＦＩＤのコードを決定するための乱数ＩＤＲを生成して偽ＲＦＩＤの各コードを決定して発信する処理がなされる。そして、ＳＧ８により、その決定された偽ＲＦＩＤをそれぞれＥＥＰＲＯＭ１９４に記憶させる処理がなされる。

【０１８０】

ブラウザフォン３０がトラップモードとなっている場合には、ＳＧ４により、ＹＥＳの判断がなされてＳＧ１０へ進み、業社の店名を受信しているか否かの判断がなされる。後述する自動決済処理等の場合には、販売業者の店名信号を受信する（ＳＨ２参照）。業社の店名を受信しておれば、制御がＳＧ１１へ進み、受信した業社に対応するトラップ型ＲＦＩＤがＶＰ用ＩＣ端末１９Ｖに記憶されているか否かの判断がなされる（図８、図９参照）。記憶されている場合にはＳＧ１２へ進み、その受信し業社に対応するトラップ型ＲＦＩＤを発信する処理がなされる。一方、ＳＧ１０またはＳＧ１２によりＮＯの判断がなされた場合には制御がＳＧ１３へ進み、図２８のＳＦ７ｂにより予め選択指定されている業者に対応するＲＦＩＤをＶＰ用ＩＣ端末１９ＶのＥＥＰＲＯＭ２６から読出して（図８

、図９参照）、そのトラップ型ＲＦＩＤを発信する処理がなされる。例えば、個人ユーザがポイントカードの発行を行なっていないスーパーマーケット等の業社内を歩いたりその業社内で購入商品を自動決済した場合等においてその業社側からＲＦＩＤ送信要求が発信された場合には、ＳＦ７ｂにより予め選択指定されている業者に対応するトラップ型ＲＦＩＤが発信されることとなる。例えば、個人ユーザがＭＴＴの業社を選択操作してＳＦ７ｂによりその選択指定された業者ＭＴＴをブラウザフォン３０に記憶させた場合において、ポイントカードを新規発行していないすなわちＶＰを登録していないスーパーマーケット（ＲＩＦに）においてＲＦＩＤ送信要求が出された場合には、ブライザフォン３０からＭＴＴに対応するトラップ型ＲＦＩＤであるｍｔｔが発信されることとなる。そのトラップ型ＲＦＩＤであるｍｔｔを発信した後、スーパーマーケットＲＩＦがトラップ型ＶＰであるＥ（Ｂ１３Ｐ）宛にダイレクトメールあるいはＥメールが送信されてきた場合には（図９参照）、業社ＭＴＴに登録されているトラップ型ＶＰの個人情報Ｅ（Ｂ１３Ｐ）、Ｅメールアドレス△△△△△等が、業社ＭＴＴからスーパーマーケットＲＩＦに不正に横流しことが分かる。このように、トラップ型ＲＦＩＤを発信することにより、後日送られてきた電子メールやダイレクトメールの宛名と送り主とをチェックすることにより、個人情報が不正に横流しされたか否かをチェックすることが可能となる。

【０１８１】

図３０は、個人ユーザが百貨店等の業社において商品を購入した後自動決済を行なう場合の決済用ゲートの通過状態を示す説明図である。百貨店（業社）２０６により個人ユーザ２０２が商品を購入して手提げ袋２０３に詰め込み、決済用の通過ゲート２０６を通過して購入商品の決済を行なう。購入商品には、それぞれにＲＦＩＤタグが付されており、通過ゲート２０６に設けられているタグリーダライタ２０１との間で交信を行なう。また、個人ユーザ２０２はブラウザフォン３０を所持している。

【０１８２】

百貨店（業社）２０６には、決済サーバ２０４とデータベース２０５とが設置されている。決済サーバ２０４は、通過ゲート２０６に設けられているタグリーダライタ２０１と電気的に接続されている。タグリーダライタ２０１は、通過ゲート２０６を通過する際に個人ユーザ２０２の所持しているブラウザフォン３０および個人ユーザ２０２の手提げ袋２０３内に収納されている購入商品に付されているＲＦＩＤタグと交信を行ない、決済に必要なデータを決済サーバ２０４へ送信する。決済サーバ２０４に接続されているデータベース２０５には、顧客データが記憶されている。具体的には、顧客名Ｅ（Ｂ１３Ｐ）、Ｅ（ＮＰＸＡ）…と、それら各顧客名に対応するポイント数、住所、Ｅメールアドレスが記憶されている。住所は、トラップ型ＶＰであるＥ（Ｂ１３Ｐ）のコンビニエンスストアの住所□×○、Ｅ（ＮＰＸＡ）のコンビニエンスストアの住所である△○○（図３参照）であり、Ｅメールアドレスは、トラップ型ＶＰの場合には金融機関７に開設しているトラップ型ＶＰ用のＥメールアドレスである△△△△△となっている（図３参照）。なお、購入商品に付されているＲＦＩＤタグは、決済用ゲートを通過して決済が完了し時点でタグリーダライタ２０１からの所定の信号（たとえば決済完了信号）を受信した初めてＲＦＩＤ発信停止状態にすることが可能となる。したがって、決済完了前においては、ＳＤ７、ＳＦ５等に従ってブラウザフォン３０からＯＦＦモード指令が発信されたとしてもＲＦＩＤ発信停止状態にはならない。

【０１８３】

図３１は、図１４のＳ１００に示された自動決済処理のサブルーチンプログラムを示すフローチャートである。ＳＨ１により、自動決済開始信号を受信したか否かの判断がなされる。個人ユーザ２０２が通過ゲート２０６を通過する際にタグリーダライタ２０１から自動決済開始信号がブラウザフォン３０に送信されて来れば、ＳＨ１によりＹＥＳの判断がなされてＳＨ２へ進み、販売業社である百貨店２０６の店名信号を受信したか否かの判断がなされ、受信するまで待機する。タグリーダライタ２０１から店名信号がブラウザフォン３０へ送信されて来れば、ＳＨ３へ進み、送信されてきた店名（業社名）に対応するトラップ型ＲＦＩＤがＶＰ用ＩＣ端末１９Ｖに既に記憶されているか否かの判断がなされ

る。既に記憶されている場合にはＳＨ５へ進み、まだ記憶されていない場合にはＳＨ４へ進み、送信されて来た店名(業社名)に対応させて新しいトラップ型ＲＦＩＤを生成してＶＰ用ＩＣ端末１９ＶをＥＥＰＲＯＭ２６に記憶させる処理がなされる。

【０１８４】

次にＳＨ５へ進み、送信されてきた店名の業社がポイントカードを発行して登録している業社であるか否かの判断がなされる。ポイントカードの登録がなされていない場合にはＳＨ１４へ進むが、ポイントカードの発行なされている業社の場合にはＳＨ６へ進み、デビッド決済、クレジットカード決済の両方が可能な旨をブラウザフォン３０により表示する処理がなされる。

【０１８５】

ＳＨ１～ＳＨ６の処理の間に、タグリーダライタ２０１は手提げ袋２０３に収納されている各購入商品に付されているＲＦＩＤタグと交信してそのＲＦＩＤタグから送信されてきた各ＲＦＩＤを決済サーバ２０４へ送信する。決済サーバ２０４は、その送信されてきた各ＲＦＩＤに対応する商品価格を割出してその合計を算出してタグリーダライタ２０１へ送信する。タグリーダライタ２０１は、その合計金額を個人ユーザ２０３のブラウザフォン３０へ送信する。

【０１８６】

次に制御はＳＨ７へ進み、払出金額を受信する処理がなされる。タグリーダライタ２０１から合計金額（払出金額）がブラウザフォン３０へ送信されてくることにより、この支払い金額の受信処理が行なわれる。次にＳＨ８へ進み、決済処理の入力操作があったか否かの判断がなされる。個人ユーザ２０２がブラウザフォン３０により決済処理を入力する。決済の種類は、前述したデビッドカード決済とクレジットカード決済とリロード金額決済とがある。リロード金額決済とは、個人ユーザ２０２の銀行口座の残額から一部ブラウザフォン３０に引き落としてブラウザフォン３０にリロードした金額を用いて決済を行なうものである。次にＳＨ９へ進み、ＳＨ７により受信された支払金額をブラウザフォン３０により表示する処理がなされる。次にＳＨ１０へ進み、その支払い金額に同意して決済を行なうためのＯＫ操作があったか否かの判断がなされる。ＯＫ操作がない場合にはＳＨ１１へ進み、決済をキャンセルするキャンセル操作があったか否かの判断がなされ、ない場合にはＳＨ１０へ戻る。このＳＨ１０、ＳＨ１１のループの巡回途中で、顧客２０２がブラウザフォン３０を操作してＯＫ操作を入力すれば制御がＳＨ１３へ進む。一方、個人ユーザ２０２がキャンセル操作を行なえばＳＨ１２へ進み、ブラウザフォン３０からタグリーダライタ２０１へキャンセル信号が発信され、商品の購入をキャンセルする意思表示が送信される。

【０１８７】

ＳＨ１３では、ＳＧ８により入力された決済の種類がリロード金額決済であるか否かの判断がなされる。リロード金額決済の場合にはＳＨ１４へ進み、ＳＨ７により受信した支払金額をブラウザフォン３０にリロードされているリロード金額との大小関係を判別し、支払金額以上のリロード金額があるか否かの判断がなされる。支払金額以上のリロード金額がある場合にはＳＨ１５によりＯＫ信号がブラウザフォン３０からタグリーダライタ２０１へ送信され、その信号が決済サーバ２０４へ送信される。次にＳＨ１６により、ＶＰ用決済処理がなされる。このＶＰ用決済処理は、図５３～図５５にその詳細が示されている。ＳＨ１６の場合にはリロード金額決済を行なうために、図５５のＳ２４９によりＹＥＳの判断がなされてＳ２５０～Ｓ２５２ｂの処理が行なわれることとなる。

【０１８８】

次にＳＨ１７により、ポイントカード加算処理が行なわれる。このポイントカード加算処理は、購入商品の合計金額に対応するポイント数をポイントカードに加算するための処理であり、図３２（ａ）に示されている。

【０１８９】

一方、ＳＨ１４によりＮＯの判断がなされた場合には、ＳＨ１８へ進み、キャンセル信号をブラウザフォン３０からタグリーダライタ２０１へ送信する処理がなされ、その信号

が決済サーバ２０４へ送信される。次にＳＨ１９へ進み、残額不足である旨の表示がブラウザフォン３０により行なわれる。

【０１９０】

なお、決済相手の業社がポイントカードを登録していない業社の場合にはＳＨ５によりＮＯの判断がなされてＳＨ１４～ＳＨ１９のリロード決済の処理が行なわれることとなり、クレジット決済やデビッド決済は行なわれない。これは、ポイントカードを登録していない業社の場合には個人ユーザ２０２のＶＰ情報をその業社に登録していないために、ＶＰとしてクレジット決済やデビッド決済を行なうことが不可能なためである。

【０１９１】

ＳＨ１３によりＮＯの判断がなされた場合にはＳＨ２０へ進み、入力された決済処理がクレジット決済であるか否かの判断がなされる。クレジット決済の場合にはＳＨ２２に進み、ＯＫ信号がブラウザフォン３０からタグリーダライタ２０１へ送信され、その信号が決済サーバ２０４へ送信される。次に、ＳＨ２３へ進み、ＶＰ用決済処理が行われる。このＳＨ２３のＶＰ用決済処理は、クレジット決済であるために、図５５のＳ２３８によりＹＥＳの判断がなされてＳ２３７～Ｓ２４８のクレジット決済処理が行なわれることとなる。

【０１９２】

入力された決済処理がデビッド決済の場合にはＳＨ２０によりＮＯの判断がなされてＳＨ２１へ進み、デビッド決済要求信号をブラウザフォン３０がタグリーダライタ２０１へ送信し、その信号が決済サーバ２０４へ送信される。決済サーバ２０４は、データベース２００を検索して決済相手の顧客名に対応するバーチャル口座番号例えばＥ（２５０３）を割出し(図３０参照)、そのバーチャル口座番号内に残額がどの程度あるかを金融機関７に問い合わせる。そして、残額が支払金額以上の場合には、ＯＫ信号をタグリーダライタ２０１を介してブラウザフォン３０へ送信する。一方、残額が支払金額未満であった場合には、ＮＧ信号をタグリーダライタ２０１を介してブラウザフォン３０へ送信する。

【０１９３】

ブラウザフォン３０では、ＳＨ２４により、ＯＫ信号を受信したか否かの判断がなされ、未だに受信していない場合にはＳＨ２６によりＮＧ信号を受信したか否かの判断がなされ、未だに受信していない場合にはＳＨ２４へ戻る。

【０１９４】

ＳＨ２４、ＳＨ２６のループの巡回途中で、タグリーダライタ２０１からＯＫ信号がブラウザフォン３０へ送信されてくれば、制御がＳＨ２５へ進み、ＶＰ用決済処理がなされる。この場合には、デビッド決済であるために、図５４（ｂ）のＳ２２０によりＹＥＳの判断がなされてＳ２３５～Ｓ２３４のデビッド決済処理が行なわれることとなる。

【０１９５】

タグリーダライタ２０１からＮＧ信号がブラウザフォン３０へ送信されてくれば、ＳＨ２６によりＹＥＳの判断がなされてＳＨ２７へ進み、ＮＧ表示がブラウザフォン３０により行なわれる。

【０１９６】

図３２（ａ）は、ＳＨ１７に示されたポイントカード加算処理のサブルーチンプログラムを示すフローチャートである。ＳＩ１により、該当するＶＰ情報を発信する処理が行なわれる。これは、決済相手の業社に登録されているＶＰをＶＰ用ＩＣ端末１９ＶのＥＥＰＲＯＭ２６から検索し、その検索されたＶＰ氏名等の情報（例えばＥ（Ｂ１３Ｐ））をタグリーダライタ２０１へ送信する。タグリーダライタ２０１は、その受信したＶＰ情報を決済サーバ２０４へ送信する。決済サーバ２０４は、受信したＶＰ氏名に基づいてデータベース２０５を検索し（図３０参照）、例えば受信した顧客名がＥ（Ｂ１３Ｐ）の場合には、現在のポイント数１９０１８を割出して、その現在のポイント数に対し、購入商品の合計金額に対応したポイント数を加算する処理を行なう。そしてその加算ポイント数を決済サーバ２０４がタグリーダライタ２０１を介してブラウザフォン３０へ送信する。

【０１９７】

ブラウザフォン３０では、ＳＩ２によりポイント受信したか否かの判断がなされ、あるまで待機する。そして、タグリーダライタ２０１から加算ポイント数を受信すれば、制御がＳＩ３へ進み、該当する業社(決済相手の業社)に対応させてＶＰ用ＩＣ端末１９ＶのＥＥＰＲＯＭ２６に記憶させる処理が行なわれる。

【０１９８】

図２３（ｂ）は、百貨店等の業社２０６においてポイントカードを新規発行して登録してもらう際のブラウザフォン３０の処理動作を示すフローチャートである。ＳＪ１により、個人ユーザ２０２がポイントカード登録操作をブラウザフォン３０により行なったか否かの判断がなされ、行なった場合にはＳＪ２へ進み、金融機関７に既に登録されているトラップ型ＶＰであって未だポイントカード登録に用いられていないトラップ型ＶＰはＶＰ用ＩＣ端末１９ＶのＥＥＰＲＯＭ２６に記憶されているか否かの判断がなされる。判断の答えがＮＯの場合にはＳＪ３へ進み、トラップ型ＶＰがない旨の表示がブラウザフォン３０により行なわれる。その際には、個人ユーザ２０２は、金融機関７に対して、新たなトラップ型ＶＰを生成して登録してもらうための処理を行なう。新たなトラップ型ＶＰの生成要求があった場合には、金融機関７のＶＰ管理サーバ９は、図３７または図４０（ｂ）のトラップ型ＶＰ処理を行なって新たなトラップ型ＶＰを生成して登録する処理を行なう。

【０１９９】

一方、ＳＪ２により常に登録されているトラップ型ＶＰであってポイントカードの登録にまだ用いられていないトラップ型ＶＰの記憶があると判断された場合には、ＳＪ４へ進み、そのトラップ型ＶＰの中から１つ選択してその住所，氏名等の必要な情報をブラウザフォン３０からタグリーダライタ２０１を介して決済サーバ２０４へ送信する処理が行なわれる。決済サーバ２０４は、受信したトラップ型ＶＰ情報に基づいてポイントカードの新規登録を行なっているか否かの判断を行ない、その判断結果をタグリーダライタ２０１を介してブラウザフォン３０へ返信する。

【０２００】

ブラウザフォン３０では、ＳＪ５により、ＯＫ信号を受信したか否かの判断を行ない、未だ受信していない場合にはＳＪ６によりＮＧ信号を受信したか否かの判断を行ない、未だ受信していない場合にはＳＪ５へ戻る。このＳＪ５、ＳＪ６のループの巡回途中で、決済サーバ２０４の判断結果としてＯＫ信号を受信すれば、ＳＪ５によりＹＥＳの判断がなされてＳＪ７へ進み、ポイントカードの登録相手である業社名を受信したか否かの判断がなされる。決済サーバ２０４は、ＯＫ信号を送信した後、当店の業社名をタグリーダライタ２０１を介してブラウザフォン３０へ送信する。すると、ＳＪ７によりＹＥＳの判断がなされてＳＪ８へ進み、その受信した業社名に対応させてトラップ型ＶＰをＶＰ用ＩＣ端末１９ＶのＥＥＰＲＯＭ２６へ記憶させる処理がなされる。

【０２０１】

一方、決済サーバ２０４からの判断結果がＮＧであった場合には、ＳＪ６によりＹＥＳの判断がなされてＳＪ９へ進み、ＮＧ表示がブラウザフォン３０により行なわれる。

【０２０２】

図３３は、販売業社２０６の決済サーバ２０４の決済処理を示すフローチャートである。ＳＫ１により、自動決済の開始であるか否かの判断がなされ、自動決済の開始でない場合にはＳＫ２に進み、ポイントカードの新規登録要求であるか否かの判断がなされ、新規登録要求でない場合にはＳＫ３へ進み、その他の処理が行なわれてＳＫ１へ戻る。

【０２０３】

個人ユーザ２０２が決済のために通過ゲート２０６を通過した場合には、ＳＫ１によりＹＥＳの判断がなされてＳＫ４へ進み、店名（業社名）の信号を決済サーバ２０４がタグリーダライタ２０１を介してブラウザフォン３０へ送信する指令処理を行なう。次にＳＫ５へ進み、ＲＦＩＤ送信要求の信号をタグリーダライタ２０１に発信させるための指令処理を行なう。次にＳＫ６へ進み、ＲＦＩＤを受信したか否かの判断がなされ、受信するまで待機する。手提げ袋２０３に収納されている各購入商品に付されているＲＦＩＤタグか

ら発信された各ＲＦＩＤがタグリーダライタ２０１に読取られてその信号が決済サーバ２０４へ送信される。すると、ＳＫ６によりＹＥＳの判断がなされてＳＫ７へ進み、受信した各ＲＦＩＤの内当店の販売商品として登録されているＲＦＩＤを検索する処理がなされる。百貨店(業社)２０６のデータベース２０５には、図３１に示した顧客データばかりでなく、販売商品の各ＲＦＩＤとそれに対応させた商品価格データが記憶されている。決済サーバ２０４は、データベース２０５を検索して、データベース２０５に登録されているＲＦＩＤ中に送信されてきたＲＦＩＤと一致するものであるか否かを判別し、一致するものを検索する。そしてＳＫ８により、その一致するＲＦＩＤの商品価格の合計を算出する処理がなされる。次に、ＳＫ９へ進み、その算出した合計金額を支払い金額としてタグリーダライタ２０１を介してブラウザフォン３０へ送信する処理が行なわれる。

【０２０４】

次にＳＫ１０へ進み、ブラウザフォン３０からＯＫ信号を受信したか否かの判断がなされ、またＳＫ１１により、ブラウザフォン３０からキャンセル信号を受信したか否かの判断がなされる。このＳＫ１０、ＳＫ１１のループの巡回途中で、ブラウザフォン３０からＯＫ信号が送信されてくればＳＫ１２により決済処理を行なう。この決済処理は、図５３～図５５のブラウザフォン３０側の決済処理動作に対応した販売業者側の決済サーバ２０４の処理動作である。次にＳＫ１３へ進み、販売された商品のＲＦＩＤをデータベース２０５の登録から抹消する処理がなされる。次にＳＫ１４へ進み、販売商品の合計金額に対応する加算ポイント数を算出する処理がなされる。

【０２０５】

ＳＫ１５へ進み、ＶＰ情報を受信したか否かの判断がなされ、受信するまで待機する。ＳＩ１に従ってブラウザフォン３０から該当するＶＰ情報が送信されて来れば、制御がＳＫ１６へ進み、加算ポイント数をタグリーダライタ２０１からブラウザフォン３０へ送信する処理がなされる。次にＳＫ１７へ進み、受信したＶＰに対応するポイントデータをデータベース２０５から割出し(図３０参照)、その割出されたポイント数に対し加算ポイント数を加算更新する処理がなされてＳＫ１へ戻る。

【０２０６】

次に、ポイントカードの新規登録要求があった場合にはＳＫ２によりＹＥＳの判断がなされてＳＫ２１へ進み、ＶＰを受信したか否かの判断がなされ、受信するまで待機する。ＳＪ４に従ってブラウザフォン３０からトラップ型ＶＰ情報が送信されてくれば、制御がＳＫ２２へ進み、金融機関７のＶＰ管理サーバ９に適正に登録されているＶＰであるか否かの問合せ処理がなされる。ＶＰ管理サーバ９では、データベース１２ａに適正に登録されているＶＰであるか否かをチェックし、そのチェック結果を販売業者２０６の決済サーバ２０４へ返信する。決済サーバ２０４では、返信されてきたチェック結果が適正であるか否かＳＫ２３により判定し、適正でない場合にはＳＫ２４によりＮＧをタグリーダライタ２０１を介してブラウザフォン３０へ返信する処理がなされる。一方、適正である場合にはＳＫ１８へ進み、ＯＫ信号をタグリーダライタ２０１を介してブラウザフォン３０へ返信する処理がなされる。

【０２０７】

ＳＫ１９へ進み、店名（業社名）をタグリーダライタ２０１を介してブラウザフォン３０へ送信する処理がなされ、ＳＫ２２により、ポイント対象顧客としてＶＰをデータベース２０５に新規登録する処理がなされる（図３０参照）。

【０２０８】

次に、ＶＰ用ＩＣ端末１９Ｖの制御動作を図３４に基づいて説明する。ＶＰ用ＩＣ端末１９Ｖは、Ｓ２５３により、暗証番号チェック処理を行なう。次にＳ２５４へ進み、トラップ型ＲＦＩＤ処理を行なう。次にＳ２５５へ進み、本人証明処理を行なう。次にＳ２５６へ進み、データ入力処理を行なう。次にＳ２５７へ進み、ユーザエージェント動作処理を行なう。次にＳ２５８へ進み、リロード金額の使用処理を行なう。次にＳ２５９へ進み、署名処理を行なう。次にＳ６１５により、トラップ型ＶＰ処理がなされる。この処理は、図３７に基づいて後述する。

【０２０９】
図３５（ａ）は、Ｓ２５３に示された暗証番号チェック処理のサブルーチンプログラムを示すフローチャートである。Ｓ２６８により、暗証番号が入力されたか否かの判断がなされ、入力されていない場合にはこのままサブルーチンプログラムが終了する。一方、暗証番号が入力されれば、Ｓ２６９へ進み、入力された暗証番号を記憶している暗証番号と照合する処理がなされる。次にＳ２７０へ進み、照合の結果一致するか否かの判断がなされ、一致しない場合にはＳ２７１へ進み、不適正な旨をブラウザフォン３０へ送信する処理がなされる。一方、一致する場合にはＳ２７２へ進み、適正な旨の返信を行なう。
【０２１０】
図３５（ｂ）は、Ｓ２５４に示されたトラップ型ＲＦＩＤ処理（ＶＰ用）のサブルーチンプログラムを示すフローチャートである。Ｓ２７３により、業社名の入力があるか否かの判断がなされる。ブラウザフォン３０はＶＰ用ＩＣ端末１９Ｖにトラップ型ＲＦＩＤに対応する業社名（店名）を入力する（ＳＧ１１、ＳＧ１３、ＳＨ３）。入力があればＳ２７４へ進み、入力された業社名に対応するトラップ型ＲＦＩＤの読出し要求か否かが判断される。ＳＧ１１、ＳＧ１３にしたがった要求の場合にはＳ２７４によりＹＥＳの判断がなされ、Ｓ２７５により、ＥＥＰＲＯＭ２６に記憶されているトラップ型ＲＦＩＤの中から入力された業社名に対応するトラップ型ＲＦＩＤを検索する処理がなされる。検索の結果対応するトラップ型ＲＦＩＤが記憶されているか否かがＳ２７６により判断される。記憶がある場合にはその対応するトラップ型ＲＦＩＤをブラウザフォン３０へ出力する処理がＳ２７７によりなされる。一方、Ｓ２７６により対応するトラップ型ＲＦＩＤの記憶がないと判断された場合には、ブラウザフォン３０へ出力する処理がなされる。
【０２１１】
ブラウザフォン３０は、記憶がない旨の信号を受信した場合には、ＳＨ３によりＮＯの判断を行ない、ＳＨ４により、業社名に対応させてトラップ型ＲＦＩＤを記憶させる指令をＶＰ用ＩＣ端末１９Ｖへ出力する。それを受けたＶＰ用ＩＣ端末１９Ｖは、Ｓ２７３によりＹＥＳＳ２７４によりＮＯの判断を行い、Ｓ２７８により、新たなトラップ型ＲＦＩＤを生成して、業社名に対応させてＥＥＰＲＯＭ２６に記憶する処理を行なう。
【０２１２】
図３５（ｃ）は、Ｓ２５５に示された本人証明処理（ＶＰ用）のサブルーチンプログラムを示すフローチャートである。Ｓ２８０により、乱数Ｒの入力があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。乱数Ｒの入力があった場合にＳ２８１へ進み、ＶＰ出生依頼時であるか否かの判断がなされる。ＶＰ出生依頼時の場合には、Ｓ６，Ｓ１５１で説明したように、ＲＰの認証鍵ＫＮを用いてＲＰが正当な本人であることを証明する必要がある。そのために、ＶＰ出生依頼時の場合にはＳ２８３進み、入力された乱数ＲをＲＰの認証鍵ＫＮで暗号化してＩを生成する処理すなわちＩ＝E_{KN}（Ｒ）の算出処理を行なう。そして、と２８４により、その算出されたＩをブラウザフォン３０へ出力する処理がなされる。
【０２１３】
一方、ＶＰ出生依頼時でない場合には、Ｓ２８１によりＮＯの判断がなされてＳ２８２へ進み、ＶＰは正当な本人であることを証明するべく、ＶＰの秘密鍵ＫＳを用いて入力された乱数Ｒを暗号化してＩを算出する処理、すなわち、Ｉ＝E_{SK}（Ｒ）を算出する処理を行なう。そしてＳ２４８により、その算出されたＩをブラウザフォン３０へ出力する処理がなされる。
【０２１４】
図３６（ａ）は、Ｓ２５６，Ｓ２６３に示されたデータ入力処理のサブルーチンプログラムを示すフローチャートである。Ｓ２９３により、データ入力があったか否かの判断がなされる。入力されるデータとしては、前述したように、ＶＰ管理サーバ９によって誕生したＶＰに関するデータが記録されているＣＤ－ＲＯＭの記録データ、ユーザエージェントの知識データ（Ｓ１７９，Ｓ１８９参照）、引落し額Ｇ（Ｓ１８１，Ｓ１９１参照）等がある。これらのデータが入力されれば、制御がＳ２９４へ進み、入力データに対応する

記憶領域に入力データを記憶させる処理がなされる。

【０２１５】

図３６（ｂ）は、Ｓ２５７，Ｓ２６４に示されたユーザエージェント動作処理のサブルーチンプログラムを示すフローチャートである。Ｓ２９５により、公開鍵出力要求があったか否かの判断がなされる。公開鍵の出力要求があった場合には、Ｓ２９８に進み、記憶している公開鍵ＫＰを出力する処理がなされる。Ｓ２９５によりＮＯの判断がなされた場合にＳ２９６へ進み、デビットカード情報の出力要求があったか否かの判断がなされる。あった場合にはＳ２９９へ進み、記憶しているデビットカード情報を出力する処理がなされる。

【０２１６】

Ｓ２９６によりＮＯの判断がなされた場合にはＳ２９７へ進み、クレジットカード情報の出力要求があったか否かの判断がなされる。あった場合にはＳ３００へ進み、記憶しているクレジットカード情報を出力する処理がなされる。次にＳ３０１へ進み、その他の動作処理が行なわれる。このその他の動作処理は、図３０に基づいて後述する。

【０２１７】

図３６（ｃ）は、Ｓ２５８，Ｓ２６５に示されたリロード金額の使用処理のサブルーチンプログラムを示すフローチャートである。Ｓ３０２により、引落し額Ｇの引落し要求があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。あった場合には、Ｓ３０３へ進み、記憶しているリロード金額がＧを減算する処理がなされ、Ｓ３０４へ進み、引落し完了信号を返信する処理がなされる。

【０２１８】

図３６（ｄ）は、Ｓ２５９により示されたＶＰ署名処理のサブルーチンプログラムを示すフローチャートである。Ｓ９９９により、メッセージダイジェストＭＤとＶＰ氏名との入力がブラウザフォン３０からあったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。

【０２１９】

ＭＤとＶＰ氏名との入力があった場合には制御がＳ９９８へ進み、その入力されたＶＰ氏名から秘密鍵（ＫＳ）を生成する処理がなされる。具体的には、ＶＰ用ＩＣ端末１９Ｖは、入力されたＶＰ氏名に基づいてトラップ型ＲＦＩＤデータ記憶領域を検索してその入力されたＶＰ氏名が本名Ｂ１３Ｐ（図９参照）を何回暗号化したものであるかを割出す。その割出された暗号化回数だけＶＰの秘密鍵をＶＰの秘密鍵で暗号化して秘密鍵（ＫＳ）を生成する。

【０２２０】

次に制御がＳ９９７へ進み、その秘密鍵（ＫＳ）を用いてメッセージダイジェストＭＤを復号化して二重署名を生成する処理がなされる。次に制御がＳ９９８へ進み、その二重署名$D_{(KS)}$（ＭＤ）をブラウザフォン３０へ出力する処理がなされる。

【０２２１】

図３７は、Ｓ６１５により示されたトラップ型ＶＰ処理のサブルーチンプログラムを示すフローチャートである。Ｓ６２０により、新たなトラップ型ＶＰの生成要求があったか否かの判断がなされ、ない場合にはＳ６２３へ進み、トラップ型ＶＰが使用済みであるか否かの問合せがあったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。

【０２２２】

ブラウザフォン３０がＳ５９８に従ってＶＰ用ＩＣ端末１９Ｖに新たなトラップ型ＶＰの生成要求を出した場合には、Ｓ６２０によりＹＥＳの判断がなされて制御がＳ６２１へ進む。Ｓ６２１では、ＶＰ用ＩＣ端末１９Ｖのトラップ型ＲＦＩＤデータ領域の最後のＶＰ氏名の暗号回数ｎを「１」加算して、ＶＰの本名をｎ＋１回秘密鍵で暗号化して新たなトラップ型ＶＰ氏名を生成する処理がなされる。たとえば図９の場合には、トラップ型ＲＦＩＤデータ領域の最後のＶＰ氏名E^3（Ｂ１３Ｐ）の暗号回数が３回であり、これに「１」加算して暗号回数４にし、ＶＰの本名Ｂ１３Ｐを４回暗号化して新たなトラップ型Ｖ

Ｐ氏名E^4（Ｂ１３Ｐ）を生成する処理がなされる。

【０２２３】

次にＳ６２２へ進み、その生成されたトラップ型ＶＰを、ブラウザフォン３０へ出力するとともに、トラップ型ＲＦＩＤ領域における最後のＶＰ氏名の次の空き領域に記憶させる処理がなされる。

【０２２４】

Ｓ５９０に従ってブラウザフォン３０がＶＰ用ＩＣ端末１９Ｖに対し今アクセスしようとしているサイト（図３０の自動決済しようとしている業社）にトラップ型ＶＰが既に使用されているか否かの問合せを行なった場合には、Ｓ６２３によりＹＥＳの判断がなされて制御がＳ６２４へ進む。この問合せの際にはブラウザフォン３０はＶＰ用ＩＣ端末１９Ｖに対し、今アクセスしようとしているサイト名（図３０の自動決済しようとしている業社名）も併せて伝送する。Ｓ６２４では、トラップ型ＲＦＩＤ領域（図９参照）を検索する処理がなされる。制御がＳ６２５へ進み、伝送されてきたサイト名（業社名）に対しトラップ型ＶＰ氏名が使用済みであるか否かの判断がなされる。たとえばブラウザフォン３０から伝送されてきたサイト名（業社名）がＭＥＣであった場合には、図９を参照して、トラップ型ＶＰ氏名E^2（Ｂ１３Ｐ）が使用済みであることがわかる。

【０２２５】

トラップ型ＶＰ氏名が使用済みであると判断された場合には制御がＳ６２６へ進み、使用済みである旨をブラウザフォン３０へ出力するとともに、Ｓ６２７により、使用されているトラップ型ＶＰとそれに対応するトラップ型ＲＦＩＤデータとをブラウザフォン３０へ出力する処理がなされる。たとえば、図９の場合には、伝送されてきたサイト名（業社名）がＭＥＣであった場合には、トラップ型ＶＰとしてE^2（Ｂ１３Ｐ）がブラウザフォン３０へ出力されるとともに、トラップ型ＲＦＩＤデータｍｅｃがブラウザフォン３０へ出力される。

【０２２６】

図９のトラップ型ＲＦＩＤ領域を検索した結果、ブラウザフォン３０から伝送されてきたサイト名（業社名）に対しトラップ型ＶＰが未だ使用されていない場合にはＳ６２５によりＮＯの判断がなされて制御がＳ６２８へ進み、未使用の旨をブラウザフォン３０へ出力する処理がなされる。

【０２２７】

図３８，図３９は、コンビニエンスストア２のサーバ１６の処理動作を説明するためのフローチャートである。Ｓ３１５により、ＶＰの氏名，Ｅメールアドレス，金融機関の名称を受信したか否かの判断がなされ、受信していない場合にＳ３１６へ進み、ＶＰが購入した商品を預かったか否かの判断がなされ、預かっていない場合にＳ３１７へ進み、商品の引取り操作があったか否かの判断がなされ、ない場合にはＳ３１８へ進み、その他の処理を行なった後Ｓ３１５へ戻る。

【０２２８】

このＳ３１５～Ｓ３１８のループの巡回途中で、決済サーバ１０が誕生したＶＰの氏名，Ｅメールアドレス，当該金融機関の名称をコンビニエンスストア２へ送信した場合には（Ｓ１８参照）、Ｓ３１５によりＹＥＳの判断がなされてＳ３１９へ進み、正当機関チェック処理がなされた後、Ｓ３２０へ進む。

【０２２９】

Ｓ３２０では、$R = D_{KP}(L)$であるか否かの判断がなされ、正当機関でない場合にはＮＯの判断がなされてＳ３２１へ進み、正当機関でない旨の警告表示がなされる。一方、正当機関である場合にはＳ３２０によりＹＥＳの判断がなされてＳ３２２へ進み、受信データをデータベース１７へ登録する処理がなされる。

【０２３０】

ユーザがＶＰとしてたとえば電子ショッピング等を行なってそのＶＰの住所であるコンビニエンスストア２に購入商品が配達されてコンビニエンスストア２がその商品を預かった場合には、Ｓ３１６によりＹＥＳの判断がなされてＳ３１６ａへ進み、該当するＶＰの

商品預かり情報のアドレス領域に商品を預かった旨の情報を記憶させる処理がなされる。その際に、当該商品の決済が済んでいるか否かの情報も併せて記憶させる。次に制御がＳ３２３へ進み、当該ＶＰのＥメールアドレスを割出し、そのＥメールアドレスへ商品を預かった旨のメールを送信する処理がなされる。ＶＰは、そのＥメールを見ることにより、コンビニエンスストアに購入商品が配達されたことを知ることができ、その商品を引取るためにそのコンビニエンスストアに出向く。

【０２３１】

ユーザがＶＰとしてコンビニエンスストア２に出向き、配達された商品を引取るための操作を行なえば、Ｓ３１７によりＹＥＳの判断がなされる。そして制御がＳ３２４へ進み、ＶＰ用ＩＣ端末１９Ｖの差込指示が表示される。それを見たユーザは、自己のＶＰ用ＩＣ端末１９Ｖを端末７３のＵＳＢポートへ差込んで接続する。すると、Ｓ３２５によりＹＥＳの判断がなされてＳ３２６へ進み、暗証番号チェック処理がなされる。ユーザは、端末７３に設けられているキーボードからＶＰ用の暗証番号を入力する。暗証番号が一致して適正であることを条件として、制御がＳ３２７へ進み、接続されているＶＰ用ＩＣ端末１９ＶからＶＰ用の氏名を呼出してそれに基づいてデータベース１７を検索する処理がなされる。そして、該当するＶＰの商品預かり情報のアドレス領域に、商品預かり情報が記録されているか否かの判断がＳ３２８によりなされる。商品預かり情報がなければＳ３２９へ進み、預かり商品がない旨が表示される。一方、商品預かり情報がある場合にはＳ３３０へ進み、電子証明書の出力要求がＶＰ用ＩＣ端末１９Ｖに対しなされる。ＶＰ用ＩＣ端末１９Ｖは、それを受けて、記憶している電子証明書をサーバ１６に出力する。すると、Ｓ３３１によりＹＥＳの判断がなされてＳ３３２へ進み、出力されてきた電子証明書内の公開鍵ＫＰを読出し、Ｓ３３３により、本人チェック処理がなされる。

【０２３２】

差込まれているＶＰ用ＩＣ端末１９Ｖは、前述したように、ＶＰ本名に対する電子証明書は格納しているものの、トラップ型ＶＰに対する電子証明書は格納しておらず、そのトラップ型ＶＰに対する電子証明書はＸＭＬストア５０に格納されている。ＶＰ本名を用いて電子ショッピング等を行なってその購入商品がコンビニエンスストア２へ届けられた場合には、Ｓ３２７に従って呼出されたＶＰ氏名はＶＰの本名となる。その場合には、Ｓ３３０の要求に従ってＶＰ用ＩＣ端末１９Ｖは電子証明書を出力することができる。その場合にＳ３３１によりＹＥＳの判断がなされて制御がＳ３３２へ進む。一方、トラップ型ＶＰ氏名を用いて電子ショッピングを行ないその購入商品がコンビニエンスストア２へ届けられた場合には、その商品をトラップ型ＶＰとしてコンビニエンスストア２へ引取りに行くこととなる。その場合には、Ｓ３２７によってＶＰ用ＩＣ端末１９Ｖから呼出されるＶＰ氏名は、トラップ型ＶＰ氏名となる。その結果、そのトラップ型ＶＰ氏名に対応する電子証明書の出力要求がＳ３３０からＶＰ用ＩＣ端末１９Ｖに対し出される。その場合には、ＶＰ用ＩＣ端末１９Ｖは、ＸＭＬストア５０から電子証明書を取り寄せる旨の指示を出力する。

【０２３３】

その出力があれば、制御がＳ６３１へ進み、ＸＭＬストア５０へアクセスして該当する電子証明書を取り寄せる処理がなされた後制御がＳ３３２へ進む。

【０２３４】

次にＳ３３４へ進み、$R = D_{KP}(I)$であるか否かの判断がなされる。正当でないなりすましのＶＰである場合には、Ｓ３３４によりＮＯの判断がなされてＳ３３５へ進み、不適正である旨が表示される。一方、適正なＶＰであった場合には、制御がＳ３３６へ進み、預かり商品番号を表示し、Ｓ３３７により、その商品に関し決済済みであるか否かの判断がなされ、決済済みの場合にはＳ３３９へ進むが、決済済みでない場合にはＳ３３８へ進み、決済処理が行なわれる。

【０２３５】

Ｓ３３９では、商品の引渡しが完了したか否かの判断がなされる。コンビニエンスストア２の店員は、Ｓ３３６により表示された預かり商品番号を見て、該当する番号の商品を

探し出し、顧客にその商品を引渡した後、商品引渡し完了操作を行なう。すると、Ｓ３３９によりＹＥＳの判断がなされてＳ３４０へ進み、データベース１７の商品預かり情報のアドレス領域を更新し、商品預かりなしの状態にした後、Ｓ３１５へ戻る。

【０２３６】

Ｓ３２６の暗証番号チェック処理は、図３９（ａ）に示されている。Ｓ３４５により、暗証番号の入力指示が表示され、ユーザが入力すればＳ３４７へ進み、その入力された暗証番号をサーバ１６に接続されているＶＰ用ＩＣ端末１９Ｖへ伝送し、その暗証番号の適否の判定結果がＶＰ用ＩＣ端末１９Ｖから返送されてくれば、Ｓ３４９へ進む。Ｓ３４９では、適正な判定結果か否かが判別され、不適正であればＳ３５０により不適正の表示を行なってＳ３１５へ戻るが、適正であればこのサブルーチンが終了して、制御がＳ３２７へ進む。

【０２３７】

Ｓ３３３の本人チェック処理は、図３９（ｂ）に示されている。Ｓ３５５により、乱数Ｒを生成してＶＰ用ＩＣ端末へ伝送する処理がなされ、チャレンジデータＲに対するレスポンスデータＩがＶＰ用ＩＣ端末から返送されてくるまで待機する。Ｉが返送されてくれば、このサブルーチンが終了する。

【０２３８】

Ｓ３３８の決済処理は、図３９（ｃ）に示されている。Ｓ３５９により、預かり商品の価格を表示する処理がなされ、Ｓ３６０へ進み、入金があるか否かの判断がなされる。ない場合にはＳ３６２へ進み、リロード金額による支払操作があったか否かの判断がなされ、ない場合にはＳ３６０へ戻る。そして、ユーザが現金による支払を行なってコンビニエンスストアの店員が入金があった旨の操作を行なえば、Ｓ３６０によりＹＥＳの判断がなされてＳ３６１へ進み、商品販売会社の口座へ入金処理を行なってこのサブルーチンプログラムが終了する。

【０２３９】

一方、ユーザがＶＰ用ＩＣ端末１９に記憶されているリロード金額を使用して支払操作を行なうべくその旨の操作がなされれば、Ｓ３６２によりＹＥＳの判断がなされてＳ３６３へ進み、価格Ｇの引落し要求をＶＰ用ＩＣ端末１９Ｖへ伝送する処理がなされる。そしてＳ３６４へ進み、ＶＰ用ＩＣ端末１９Ｖから引落し完了信号が出力されてきたか否かの判断がなされ、出力されてくるまで待機する。そして、引落し完了信号を受信すれば、Ｓ３６４によりＹＥＳの判断がなされてＳ３６１へ進む。

【０２４０】

次に、別実施の形態を説明する。この別実施の形態は、ブラウザフォン３０やユーザのパーソナルコンピュータ等のユーザ側端末およびＩＣ端末１９およびＷｅｂサイト（業社）によって、個人情報保護のシステムが完結する簡易型システムである。前述した実施の形態との相違は、トラップ型ＶＰのＥメールアドレスがＶＰ本名のＥメールアドレスと同じである。よって、トラップ型ＶＰ宛のＥメールを金融機関７が転送する必要がない。またトラップ型ＶＰの氏名は、そのトラップ型ＶＰがアクセスするサイト（業社）の名称を、ＶＰ本名に用いられる秘密鍵で暗号化したものを用いる。トラップ型ＶＰの口座番号やクレジット番号も、ＶＰが本名として用いる口座番号，クレジット番号と同じものを用いる。

【０２４１】

図４０（ａ）は、ＶＰ用ＩＣ端末１９ＶのＥＥＰＲＯＭ２６のトラップ型ＲＦＩＤ領域に格納されている情報を示す図である。このトラップ型ＲＦＩＤ領域には、ＶＰ氏名として、ＶＰの本名Ｂ１３Ｐのみが記憶され、トラップ型ＶＰ氏名は何ら記憶されない。トラップ型ＶＰの氏名は、トラップ型ＶＰとしてアクセスしたサイト（業社）を本名のＶＰの秘密鍵ＫＳＢで暗号化したものを用いる。この暗号化回数は１回に限らず２回以上の或る定められた回数であってもよい。よって、トラップ型ＶＰがアクセスしたサイト名（業社名）のみを記憶させることにより、そのサイト名（業社名）に対応するトラップ型ＶＰの氏名は、わざわざ記憶させなくとも、E_{KSB}（業社名）の演算式に従って必要に応じて

その都度算出することができる。トラップ型ＶＰの秘密鍵は、トラップ型ＶＰに対応するサイト名（業社名）を本名のＶＰの秘密鍵ＫＳＢで復号化したものを用いる。よって、トラップ型ＶＰに対応させて逐一公開鍵や秘密鍵をＶＰ用ＩＣ端末１９Ｖに記憶させる必要はなく、秘密鍵＝D_{KSB}（業社名）の演算式に従って必要に応じてその都度算出することができる。よって、ＸＭＬストア５０の「暗号回数」の記憶が不要となる。

【０２４２】

図４０（ｂ）は、トラップ型ＶＰ処理のサブルーチンプログラムを示すフローチャートである。このサブルーチンプログラムは、図３７に示したトラップ型ＶＰ処理の別実施の形態である。Ｓ９６０により、新たなトラップ型ＶＰの生成要求がブラウザフォン３０からあったか否かの判断がなされ、あった場合には制御がＳ９５９へ進み、アクセスするサイト（業社名）の名称の入力要求がブラウザフォン３０へ出される。ブラウザフォン３０からアクセスするサイト（業社）の名称が伝送されてくれば、制御がＳ９５７へ進み、その伝送されてきたサイト名（業社名）をＶＰの本名Ｂ１３Ｐの秘密鍵ＫＳＢで暗号化して、新たなトラップ型ＶＰ氏名であるE_{KSB}（業社名）を算出する処理がなされる。次に制御がＳ９５６へ進み、その算出した新たなトラップ型ＶＰ氏名をブラウザフォン３０へ出力する処理がなされ、Ｓ９５４により、入力されたサイト名（業社名）をトラップ型ＲＦＩＤ領域に記憶させる処理がなされる。

【０２４３】

Ｓ９５３～Ｓ９４８は、図３７に示したＳ６２３～Ｓ６２８と同じ制御のために、説明の繰返しを省略する。

【０２４４】

図４０（ｃ）は、ＶＰ用ＩＣ端末１９Ｖによって行なわれる個人情報流通チェックのサブルーチンプログラムを示すフローチャートである。Ｓ９７０により、Ｅメールの受信があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。トラップ型ＶＰ宛のＥメールの受信があれば、ブラウザフォン３０は、そのＥメールデータをＶＰ用ＩＣ端末へ入力する。すると制御がＳ９６９へ進み、その入力されたＥメールの宛名をＶＰの本名に用いられる公開鍵ＫＰＢで復号化するD_{KPB}（宛名）の演算を行ない、その演算結果がＥメールの送信者名と一致するか否かの判断がなされる。

【０２４５】

Ｅメールの宛名はトラップ型ＶＰ氏名となっており、そのトラップ型ＶＰ氏名は、そのトラップ型ＶＰがアクセスしたサイト名（業社名）をＶＰの秘密鍵ＫＳＢで暗号化したものを用いている。よって、トラップ型ＶＰがその氏名を用いてアクセスしたサイト（業社）からそのトラップ型ＶＰ宛にＥメールが送信された場合には、Ｓ９６９によりＹＥＳの判断がなされる筈である。その場合には、Ｓ９６８により、適正である旨がブラウザフォン３０へ出力され、ブラウザフォン３０の表示部７６によりその旨が表示される。一方、トラップ型ＶＰがその氏名を用いてアクセスしたサイト（業社）以外のサイト（業社）からそのトラップ型ＶＰ氏名をＥメールの宛名としてＥメールが送信されてくれば、Ｓ９６９によりＮＯの判断がなされ、制御がＳ９６７へ進む。Ｓ９６７では、Ｅメールの宛名を本名のＶＰの公開鍵ＫＰＢで復号化する処理がなされる。その結果、Ｅメールの宛名であるトラップ型ＶＰ氏名が公開鍵ＫＰＢで復号化されて平文のサイト名（業社名）が算出されることとなる。このサイト名（業社名）は、Ｅメールの宛名に用いられているＶＰ氏名としてアクセスしたサイト名（業社名）のことであり、アクセスしたサイト（業社）が個人情報をＥメールの送信者に不正流通したことが考えられる。よって、Ｓ９６７により、D_{KPB}（宛名）が不正流通し、送信者名の業者が不正入手した旨をブラウザフォン３０へ出力する。ブラウザフォン３０では、その旨を表示部７６により表示させる。

【０２４６】

図４１は、購入済商品に付されているＲＦＩＤタグから発信されるＲＦＩＤを利用したサービスを行なうのに必要となる各業社からなる構成を示す構成図である。このＲＦＩＤを利用したサービス（以下「ＲＦＩＤサービス」と言う）は、前述したサプライヤ群Ｓの１つである商品メーカー３００と、会社群４５の１つである中間流通業者３０１と、会社

群４５の一つである商品情報サービス業社３０２と、加盟店群６の１つである小売店２０ｂとにより提供可能となる。

【０２４７】

商品メーカー３００には、Ｗｅｂサーバ３０３とＷｅｂデータベース３０４とが設置されている。中間流通業者３０１には、Ｗｅｂサーバ３０５とＷｅｂデータベース３０６とが設置されている。商品情報サービス業社３０２には、Ｗｅｂサーバ３０７とＷｅｂデータベース３０８とが設置されている。小売店２０ｂには、Ｗｅｂサーバ３０９とＷｅｂデータベース３１０とが設置されている。これら各Ｗｅｂサーバ３０３、３０５、３０７、３０９等が広域・大容量中継網４３によりそれぞれ通信可能に構成されている。またＲＦＩＤサービスを受ける個人ユーザの自宅４７が広域・大容量中継網４３に接続されている。

【０２４８】

図４２は、商品情報サービス業社３０２のＷｅｂデータベース３０８に記憶されているデータの内容を示す図である。Ｗｅｂデータベース３０８には、ＲＦＩＤタグメーカーが製造したＲＦＩＤタグから発信されるＲＦＩＤを記憶するエリアと、商品メーカー３００や農産物を生産する農家等の生産者のＵＲＬを記憶するエリアと、中間流通業者３０１のＵＲＬを記憶するエリアと、小売店２０ｂのＵＲＬを記憶するエリアと、個人ユーザ（購入者）専用のページを記憶するエリアとが設けられている。

【０２４９】

図４２の場合には、ＲＦＩＤタグメーカーが製造したＲＦＩＤタグから発信されるＲＦＩＤとして、８９２０１３９６０～８９２０１４９９０が登録されている。そのうち、ｈｔｔｐ／／ｗｗｗ・ｓａｔｏのＵＲＬの生産者の各生産品に付されるＲＦＩＤタグとして、８９２０１３９６０～８９２０１４５６０が割振られている。ｈｐｐｔ／／ｗｗｗ・ｉｓｉｄａの生産者、ｈｔｔｐ／／ｗｗｗ・ｋａｔｏの生産者も、図４２に示すＲＦＩＤが割り振られている。

【０２５０】

ｈｔｔｐ／／ｗｗｗ・ｋａｎｅｉの中間流通業者には、ｈｔｔｐ／／ｗｗｗ・ｓａｔｏの生産者とｈｈｔｐ／／ｗｗｗ・ｉｓｉｄａの生産者からの生産品が入荷される。その入荷された段階で、両生産者の生産品に付されているＲＦＩＤタグから発信されるＲＦＩＤ８９２０１３９６０～８９２０１４８０１に対応して中間流通業者ｈｔｔｐ／／ｗｗｗ・ｋａｎｅｉのＵＲＬが記録される。ｈｔｔｐ／／ｗｗｗ・ｍｉｔｕｉの中間流通業者も同様に、ｈｔｔｐ／／ｗｗｗ・ｋａｔｏの生産者からの生産品が入荷され、その生産品に対応するＲＦＩＤ８９２０１４８０２～８９２０１４９９０に対応するエリアに記憶される。

【０２５１】

中間流通業者から小売店に商品が入荷されれば、その入荷された商品に付されているＲＦＩＤタグに対応するＲＦＩＤに対応してその小売店のＵＲＬが図示するように記憶される。尚、ＲＦＩＤ８９２０１４８０２～８９２０１４９９０に関しては、小売店の記憶エリアに何らＵＲＬが記憶されていない。これは、これらのＲＦＩＤを発信するＲＦＩＤタグが付された商品がまだ小売店に入荷されていない流通段階であるためである。

【０２５２】

購入者ページには、ＲＦＩＤタグが付された商品を購入した購入者のＶＰ名Ｂ１３Ｐ、ＮＰＸＡ、ＩＱＸ３等のＶＰ情報と、それに対応してＶＰが書込んだ種々の情報とが記憶される。なお、本実施の形態においては、ＩＰｖ６を用いる。

【０２５３】

図４３は、商品情報サービス業社３０２のＷｅｂサーバ３０７の制御動作を示すフローチャートである。ＳＲ１により、検索式を受信したか否かの判断がなされる。この検索式は、個人ユーザが商品を検索するためにブラウザフォン３０等から入力してＷｅｂサーバ３０７へ送信して来る検索式のことである。検索式が送信されてきていない場合にはＳＲ２へ進み、新ＲＦＩＤの登録要求があったか否かの判断がなされる。ＲＦＩＤタグのメー

カーが新たなＲＦＩＤタグを製造してそのＲＦＩＤを商品情報サービス業社３０２のＷｅｂデータベースに登録すべく登録要求をＷｅｂサーバ３０７へ送信すれば、ＳＲ２によりＹＥＳの判断がなされてＳＲ１０へ進み、その送信されて来た新ＲＦＩＤをＷｅｂデータベース３０８へ登録する処理がなされる。

【０２５４】

商品メーカー３００や農産物を生産する生産者から、自己の生産品に付するＲＦＩＤタグのＲＦＩＤを割り振ってもらうための申し込みがあったか否かの判断がＳＲ３によりなされ、あった場合にはＳＲ１１へ進み、割り振りの申し込み個数だけＲＦＩＤを生産者に割り振って発行する処理がなされる。次にＳＲ１２へ進み、その割り振ったＲＦＩＤに対応させて生産者のＵＲＬをＷｅｂデータベースに記憶して登録処理がなされる。これにより、図４２に示した商品ホームページには、記憶された生産者のＵＲＬが掲載されて表示されることとなる。

【０２５５】

中間流通業者３０１からＲＦＩＤの申し込みがあったか否かがＳＲ４により判断される。生産者が生産した生産品が中間流通業者３０１に入荷された場合にその入荷された商品に付されているＲＦＩＤタグのＲＦＩＤを中間流通業者３０１が読みって、そのＲＦＩＤを商品情報サービス業社３０２のＷｅｂサーバ３０７へ送信する。すると、ＳＲ４によりＹＥＳの判断がなされてＳＲ１３へ進み、その送信されてきたＲＦＩＤに対応させて中間流通業者は３０１のＵＲＬをＷｅｂデータベース３０８に記憶して登録する処理がなされる。その結果、図４２に示された商品ホームページに、その中間流通業者のＵＲＬが掲載されて表示されることとなる。

【０２５６】

小売店２０ｂからＲＦＩＤの申し込みがあったか否かがＳＲ５により判断される。中間流通業者３０１から商品が小売店２０ｂに入荷され、小売店２０ｂによりその入荷商品に付されているＲＦＩＤタグのＲＦＩＤが読取られてそのＲＦＩＤがＷｅｂサーバ３０７へ送信されれば、ＳＲ５によりＹＥＳの判断がなされてＳＲ１４へ進み、その送信されてきたＲＦＩＤに対応させて小売店のＵＲＬをＷｅｂデータベース３０８へ登録する処理がなされる。その結果、図４２の商品ホームページにその小売店のＵＲＬが掲載されて表示されることとなる。

【０２５７】

ＳＲ５によりＮＯの判断がなされた場合には図４４のＳＲ６へ進む。ＳＲ６により、購入者からの書込み要求があったか否かの判断がなされる。あった場合には、ＳＲ１５へ進み、正当期間証明処理がなされる。この正当期間証明処理の詳細は、図２４（ｂ）に示されている。次に、ＳＲ１６へ進み、本人確認処理を行なう。この本人確認処理の詳細は、例えば、図１８のＳ４１２～Ｓ４１７と同様の処理である。次にＳＲ１７へ進み、本人確認処理の結果正しいことの確認ができたか否かの判断がなされ、確認できない場合にはＳＲ１８により拒絶処理を行なった後ＳＲ１へ戻る。正しい確認ができた場合にはＳＲ１９へ進み、ＲＦＩＤの送信要求を個人ユーザのブラウザフォン３０へ伝送する処理がなされる。個人ユーザは、自己が購入した商品に付されているＲＦＩＤタグからＲＦＩＤを読取り、それをブラウザフォン３０からＷｅｂサーバ３０７へ送信する。すると、ＳＲ２０によりＹＥＳの判断がなされてＳＲ２１へ進み、その送信されてきたＲＦＩＤに対応する購入者ページを作成して商品ホームページに掲載するとともに、その作成された購入者ページに対応する箇所に当該個人ユーザによるメッセージ等の書込みを許容する処理がなされる。個人ユーザは、自己のＶＰ名、ＶＰの住所（コンビニエンスストアの住所）、ＶＰのＥメールアドレス等のＶＰ情報を書込むことができる。その他として、そのＲＦＩＤに対応する購入商品の使用後の感想等、当該商品を中古品として販売したい旨のメッセージ、当該商品を他の個人ユーザの商品と物々交換したい旨のメッセージ等が考えられる。使用後の感想が書きこまれることによって、他の一般消費者が商品購入の際に、その感想を参考にして判断することができると共に、その商品のメーカーが次の商品を開発する際にその感想等を参考にして商品開発をすることが可能となる。更に他の例としては、商品の購

入者が、購入者ページを商品に関するメモ代わりに利用することが考えられる。例えば、炊飯器で炊き込み御飯を炊いた時に少し水の分量が多かった場合に、その炊飯器に対応するＲＦＩＤの購入者ページの欄に、「米と水の比を４：５にして炊き込み御飯を炊いたが、少し水の分量が多かった」旨を書込んでおき、次回の炊き込み御飯を炊く時の参考にできるようにする。

【０２５８】

更なる他の例としては、商品の取り扱い説明書、契約書、保証書等の情報をその対応するＲＦＩＤを購入者ページに記憶させておいてもよい。

【０２５９】

ＳＲ６によりＮＯの判断がなされた場合にはＳＲ２３へ進み、生産者からの追加情報書込みの要求があったか否かの判断がなされる。生産者は、販売された商品に関して、そのバージョンアップ情報、付属商品の出荷情報、メーカー側が欠陥を発見した場合の欠陥通知情報等を追加情報として生産者自身のホームページに掲載する。そして、自己のホームページに商品の追加情報を掲載したことを図４２の商品ホームページに掲載してもらうべく、生産者は、Webサーバ３０７へ追加情報の書込み要求を送信する。するとＳＲ２３によりＹＥＳの判断がなされてＳＲ２４へ進み、追加情報が掲載された旨を商品ホームページに掲載する処理がなされる。また、商品が例えばパーソナルコンピュータのソフトであった場合に、そのソフトのバージョンアップ情報やバージョンアップされたソフトを有償または無償でダウンロードできるようにホームページに掲載してもよい。

【０２６０】

消費者から商品ホームページを閲覧したい旨の要求がWebサーバ３０７に送信された場合には、ＳＲ７によりＹＥＳの判断がなされてＳＲ２２へ進み、図４２に示された商品ホームページを表示する処理がなされる。その商品ホームページを閲覧した消費者は、例えば図４２に示すＲＦＩＤ８９２０１３９６０の商品について生産者から商品情報を入手したい場合には、ｈｔｔｐ／／ｗｗｗ．ｓａｔｏの生産者URLをクリックする。すると生産者のホームページに自動的にアクセスでき、ＲＦＩＤ８９２０１３９６０に対応する商品に関する種々の商品情報を閲覧することが可能となる。例えば、その商品が農産物等の食材の場合には、その食材の各種料理方法、栄養、カロリー、体への効用、生産農家、使用農薬、生産農家からのメッセージ等を閲覧できる。また、生産農家において、田植え代金や果樹園でのぶどう狩りや梨狩り体験等のイベント企画をホームページに掲載して消費者が閲覧できるようにする。

【０２６１】

個人ユーザが商品の検索を行なうべくブラウザフォン３０から商品検索用の検索式を入力してWebサーバ３０７へ送信すれば、ＳＲ１によりＹＥＳの判断がなされてＳＲ８へ進み、送られてきた検索式に従ってWebデータベース３０８を検索する処理がなされ、その検索結果をＳＲ９により個人ユーザのブラウザフォン３０へ返信する処理がなされる。ブラウザフォン３０から送信されてくる検索式は、例えば、商品種類の指定、商品生産者の指定、性能(機能)の指定等を特定するものであり、その検索式に従ってＳＲ８により、条件を満たす商品を割出してその商品情報とその商品に対応するＲＦＩＤ等をＳＲ９により返信する。商品の検索に際しては、購入者ページ(図４２参照)に書込まれている商品購入者の使用後の感想等も商品検索の一情報として利用される。更に、送られてくる検索式中には、その商品が販売されているまたは販売される予定の小売店を指定するデータも含まれている。そして、その検索式の条件を満たす商品のＲＦＩＤ全てを個人ユーザのブラウザフォン３０へ返信する。

【０２６２】

図４５は、個人ユーザのブラウザフォン３０により商品を検索して購入するためのプログラムを示すフローチャートである。ＳＱ１により、個人ユーザがブラウザフォン３０から商品検索操作を行なったか否かの判断がなされる。行なった場合にはＳＱ２へ進み、商品を検索するための検索式の入力受付処理が行われる。個人ユーザは、ブラウザフォン３０のキーを操作して商品検索式を入力する。次にＳＱ３へ進み、その入力した検索式を

Webサーバへ送信する処理が行なわれる。次に、ＳＱ４へ進み、検索結果がWebサーバ３０７から返信されてきたか否かを判断し、返信されてくるまで待機する。

【０２６３】

Webサーバ３０７により検索結果が返信されて来ればＳＱ５へ進み、その検索結果をブラウザフォン３０により表示する処理がなされる。次にＳＱ６へ進み、個人ユーザが再検索操作を行なったか否かの判断がなされる。個人ユーザは、返信されてきた検索結果を見て、それに満足しない場合には再度検索式を変更する等して再検索操作を行なう。すると、ＳＱ２からＳＱ５の処理が繰り返し行なわれることとなる。

【０２６４】

次にＳＱ７へ進み、返信されてきた検索結果に含まれているＲＦＩＤの内のいずれかをブラウザフォン３０に記憶させるための操作が行なわれたか否かの判断がなされる。個人ユーザが返信されてきた商品中に気に入った物がありかつその商品が自己の希望する小売店（最寄りの小売店等）により販売されている場合または販売される予定の場合には、その商品に対応するＲＦＩＤをブラウザフォン３０に記憶させる操作を行なう。すると、ＳＱ８へ進み、その指定されたＲＦＩＤをブラウザフォンがＥＥＰＲＯＭ１９４に記憶する処理を行なう。そして、個人ユーザは、その商品が売られている小売店に出向いて、ブラウザフォン３０に記憶されているＲＦＩＤと一致するＲＦＩＤが発信されるＲＦＩＤタグが付されている商品を探し出して購入する。このようなＲＦＩＤに基づいて小売店で商品を探し出す方法としては、小売店２０ｂのWebサーバ３０９へその記憶しているＲＦＩＤを送信し、Webサーバ３０９によりそのＲＦＩＤに対応する商品が陳列されている場所を割出して個人ユーザにその場所を知らせる。そして個人ユーザがその場所に出向き、そこに陳列されている商品のＲＦＩＤを読取って記憶しているＲＦＩＤと照合して一致するか否かを逐一判別する方法を採用する。

【０２６５】

一方、返信されてきた検索結果中に含まれている商品の何れかを個人ユーザが気に入ってその商品をその製品の生産者から直接購入したい場合には、直接購入操作をブラウザフォン３０により行なう。すると、ＳＱ９によりＹＥＳの判断がなされてＳＱ１０へ進み、その商品の生産者のホームページにアクセスする処理がなされる。次にＳＱ１１に進み、正当期間チェック処理が行なわれる。この正当期間チェック処理の詳細は、図５０（ａ）に基づいて後述する。次にＳＱ１２へ進み、正当期間チェック処理の結果その商品の生産者から送信されてきた乱数Rを受信した電子証明書内の公開鍵KPを用いて算出された$D_{KP}(L)$とが一致するか否かの判断がなされる。一致しない場合にはＳＱ１４により、正当期間でない旨の警告表示がブラウザフォン３０によりなされる。一方、一致する場合にはＳＱ１３により、本人証明処理が行なわれた後ＳＱ１５へ進む。この本人証明処理は、例えば図３５（ｃ）にその詳細が示されている。

【０２６６】

ＳＱ１５では、個人ユーザのＶＰ情報を生産者（商品メーカー）３００のWebサーバ３０３へ送信する処理がなされる。このＶＰ情報は、ブラウザフォン３０に装着されているＶＰ用ＩＣ端末１９ｂのＥＥＰＲＯＭ２６に記憶されているＶＰ氏名・住所、ＶＰのＥメールアドレス等である。次にＳＱ１６へ進み、購入したい商品に対応するＲＦＩＤを指定して直接購入を申し込む旨の情報をWebサーバ３０３へ送信する。次にＳＱ１７へ進み、ＶＰ用決済処理がなされる。このＶＰ用決済処理の詳細は、図５３に示されている。この決済処理が終わった後、商品の生産者はＲＦＩＤにより指定された商品をＶＰ（コンビニエンスストアの住所）へ配送する。個人ユーザは、そのコンビニエンスストアに出向いてＶＰとしてその商品を引取る。

【０２６７】

返信されてきた検索結果中に気に入った商品がありその商品を予約購入したい場合には、個人ユーザはブラウザフォン３０によりＲＦＩＤを指定して購入予約操作を行う。この購入予約は、商品の生産者（商品メーカー）３００に対して商品の購入を事前に予約しておくためのものである。購入予約操作があった場合にはＳＱ２０へ進み、小売店の指定操

作があったか否か判断され、あるまで待機する。個人ユーザがブラウザフォン３０により、商品を購入したい小売店（最寄りの小売店等）を指定する操作を行えば、ＳＱ２１へ進み、希望する商品の生産者のホームページにアクセスする処理がなされる。次にＳＱ２２～ＳＱ２５の前述と同様の正当期間をチェックする処理がなされる。ＳＱ２４による本人証明処理が行われた後ＳＱ２６に進み、購入予約したいＲＦＩＤを指定された小売店等を生産者（商品メーカー）３００のWebサーバ３０３へ送信する処理が行われる。次にＳＱ２７へ進み、指定された小売店での価格を受信したか否かの判断がなされ、受信するまで待機する。後述するように、商品メーカー３００のWebサーバ３０３は、購入予約したいＲＦＩＤと購入希望の小売店とを受信すれば、その小売店での販売価格を割出してブラウザフォン３０へ返信する。すると、ＳＱ２８へ進み、受信した価格をブラウザフォン３０により表示する処理がなされ、ＳＱ２９により購入ＯＫの操作がなされたか否かの判断がなされ、なされていない場合にはＳＱ３３により購入キャンセルの操作がなされたか否かの判断がなされ、なされていない場合にはＳＱ２９に戻る。このＳＱ２９，ＳＱ３０のループの巡回途中で、個人ユーザがブラウザフォン３０により購入ＯＫの操作を行えば、ＳＱ３１へ進み、購入予約時に指定したＲＦＩＤをブラウザフォン３０のＥＥＰＲＯＭ１９４に記憶する処理がなされる。個人ユーザは、希望する商品が指定した小売店に入荷されたか否かを図４２の商品ホームページを閲覧することにより知ることができる。また、ＲＦＩＤにより指定された商品が指定された小売店に入荷された時点で商品情報サービス業社３０２のWebサーバ３０７からその個人ユーザのブラウザフォン３０へ小売店に入荷した旨の情報を送信して個人ユーザに知らせるようにしてもよい。一方、個人ユーザがブラウザフォン３０により購入キャンセル操作を行えば、ＳＱ３１を行うことなくこのサブルーチンプログラムは終了する。

【０２６８】

個人ユーザが中古品の入手を希望する場合にその旨の操作をブラウザフォン３０により行えば、ＳＱ１９によりＹＥＳの判断がなされてＳＱ３２へ進み、該当する購入者ページ(図４２参照)にアクセスする処理がなされる。次にＳＱ３３へ進み、物々交換希望であるか否かの操作をブラウザフォン３０により行う。物々交換の場合にはＳＱ３５へ進み、自己が所有している交換したい商品のＲＦＩＤをブラウザフォン３０により読取ってそれを送信する処理がなされる。そのＲＦＩＤを受信した個人ユーザは、そのＲＦＩＤをWebサーバ３０７へ送信して商品ホームページを検索し、該当する生産者のホームページにアクセスする等して商品情報を入手する。そして交換するか否かを返信する。交換する場合即ち取引きが成立する場合にはＳＱ３６によりＹＥＳの判断がなされてＳＱ３７により物々交換処理を行う。

【０２６９】

一方、物々交換ではなく有償による中古品の購入をブラウザフォン３０により入力した場合には、ＳＱ３３によりＮＯの判断がなされてＳＱ３４へ進み、有償による購入処理が行われる。

【０２７０】

図４７は、生産者（商品メーカー）３００のWebサーバ３０３の制御動作を示すフローチャートである。ＳＳ１により、アクセスがあったか否かの判断がなされる。アクセスがあった場合にはホームページを表示する。次にＳＳ３へ進み、予約購入要求があったか否かの判断がなされる。ない場合にはＳＳ４へ進み、直接購入要求があったか否かの判断がなされる。ない場合にはＳＳ２０へ進みその他の処理がなされる。

【０２７１】

前述したＳＱ１８による予約購入の要求がブラウザフォン３０から送信されてくれば、制御がＳＳ５へ進み、前述と同様の正当期間証明処理がなされ、次にＳＳ６へ進み、前述と同様の本人確認処理がなされ、ＳＳ７により本人確認の結果正しいか否かの判断がなされる。正しくない場合にはＳＳ８による拒絶処理がなされる。一方、正しい場合にはＳＳ９へ進み、ＲＦＩＤと小売店との受信があったか否かの判断がなされ、あるまで待機する。ブラウザフォン３０から前述のＳＱ２６による購入予約したいＲＦＩＤと購入希望の小

売り店とが送信されてくれば、ＳＳ１０へ進み、その小売店への直接出荷個数に達しているか否かの判断がなされる。その小売店に出荷する商品個数がある程度の量に達している場合には、中間流通業者を省いて商品メーカー３００から直接小売店に商品を出荷できる。その直接出荷個数に達しているか否かの判断がこのＳＳ１０によりなされる。達している場合にはＳＳ１１へ進み、中間流通業社を省いた直接小売店への出荷に基づく価格をブラウザフォン３０に返信する。一方、ＳＳ１０により直接出荷個数に達していないと判断された場合にはＳＳ１２へ進み、中間流通業者を省くのに必要な予約個数、現在の予約個数、中間流通業者を省いた価格及び省かなかった価格をブラウザフォン３０に返信する。

【０２７２】

前述のＳＱ９に従った直接購入の要求がブラウザフォン３０から送信されてくれば、前述と同様のＳＳ１３による正当機関証明書処理がなされ、ＳＳ１４による本人確認処理がなされ、ＳＳ１５による正しいか否かの判断がなされ、正しくなければＳＳ１６による拒絶処理がなされ、正しい場合にはＳＳ１７へ進む。

【０２７３】

ＳＳ１７では、ＶＰ情報とＲＦＩＤを受信したか否かの判断がなされ、受信するまで待機する。前述したＳＱ１５によるＶＰ情報が送信されＳＱ１６によるＲＦＩＤがブラウザフォン３０から送信されてくれば、制御がＳＳ１８へ進み、その送信されてきたＲＦＩＤに対応する商品の決済処理を行う。次にＳＳ１９により、商品をＶＰの住所（コンビニエンスストアの住所）へ配達するための処理がなされる。

【０２７４】

図４８は、Ｓ５８５により示された住所，氏名，Ｅメールアドレスの送信処理のサブルーチンプログラムを示すフローチャートである。この処理は、前述の自動決済処理（図３１参照）の際に業者側からＶＰ情報の送信要求があった場合等に実行される。Ｓ７００により、業社側から住所，氏名，Ｅメールアドレスの送信要求があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。あった場合には制御がＳ７０１へ進み、その業社に使用しているＶＰの氏名，住所，Ｅメールアドレスを送信する処理がなされる。たとえば図９に示す例の場合には、業社ＭＴＴに使用しているＶＰ氏名はＥ（Ｂ１３Ｐ）であるために、この氏名Ｅ（Ｂ１３Ｐ）を送信する。住所は、Ｂ１３Ｐの住所すなわち□△○である（図３参照）。Ｅメールアドレスは、金融機関７がトラップ型ＶＰ用として開設しているＥメールアドレス△△△△△が送信される。

【０２７５】

図４９はＳ１０１に示されたＶＰ出生依頼処理のサブルーチンプログラムを示すフローチャートである。このＶＰ出生依頼は、ＰＶを新たに誕生させるための依頼をＶＰ管理サーバ９へ出すための処理である。Ｓ１４０により、暗証番号のチェック済みであるか否かの判断がなされ、適正な暗証番号である旨のチェックが済んでいる場合にはＳ１４１へ進むが、適正な暗証番号のチェックが未だ済んでいない場合にはこのサブルーチンプログラムが終了する。適正な暗証番号である旨のチェックが済んでいる場合にはＳ１４１へ進みＶ出生要求の操作があったか否かの判断がなされる。ユーザがブラウザフォン３０のキーボードを操作してＶＰ出生要求の操作を行なえば、制御がＳ１４２へ進み、ＶＰ出生依頼要求を金融機関７のＶＰ管理サーバ９へ送信する処理がなされる。次にＳ１４３へ進み、正当機関チェック処理がなされる。この正当機関チェック処理は、相手側の機関（この場合には金融機関７）が正当な機関であるか否かをチェックするものであり、金融機関７になりすまして対応する不正行為を防止するためのものであり、図５０（ａ）にそのサブルーチンプログラムが示されている。

【０２７６】

先に、図５０（ａ）に基づいて正当機関チェック処理のサブルーチンプログラムを説明する。この正当機関チェック処理は、図２４（ｂ）に示された正当機関証明処理に対応するチェック側のプログラムである。まずＳ１６０により、電子証明書を受信したか否かの判断を行ない、受信するまで待機する。正当機関証明処理では、図２４（ｂ）に示されているように、Ｓ９０により電子証明書が送信される。この電子証明書が送信されてくれば

、制御がＳ１６１へ進み、乱数Ｒを生成して送信する処理がなされる。すると、機関側では、図２４（ｂ）に示すようにＳ９２により、当該機関の秘密鍵ＳＫを用いて受信した乱数Ｒを暗号化してＬを算出して送信する処理が行なわれる。このＲの暗号化データＬをブラウザフォン３０が受信すれば、制御がＳ１６３へ進み、受信した電子証明書内の公開鍵ＫＰを用いてＬを復号化する処理すなわちD_{KP}（Ｌ）を算出する処理が行なわれる。

【０２７７】

そして、図４９のＳ１４４へ進み、Ｒ＝D_{KP}（Ｌ）であるか否かの判断がなされる。正当な機関である場合には、Ｒ＝D_{KP}（Ｌ）となるはずであり、その場合にはＳ１４６へ進むが、他人が金融機関７になしすましている場合には、Ｓ１４４によりＮＯの判断がなされ、Ｓ１４５へ進み、正当機関でない旨の警告表示がブラウザフォン３０によりなされてこのサブルーチンプログラムが終了する。

【０２７８】

正当機関であることが確認された場合には、Ｓ１４６へ進み、ＲＰの氏名，住所の入力要求を受信したか否かの判断がなされ、受信するまで待機する。ＶＰ管理サーバ９では、前述したように、ＶＰ出生依頼要求を受信すれば、ＲＰの氏名，住所の入力要求を送信するのであり（Ｓ２参照）、そのＲＰの氏名，住所の入力要求をブラウザフォン３０が受信すれば、Ｓ１４６によりＹＥＳの判断がなされて制御がＳ１４７へ進む。

【０２７９】

Ｓ１４７では、ＲＰの氏名，住所の入力指示をブラウザフォン３０のディスプレイに表示する処理がなされ、入力があるまで待機する（Ｓ１４８）。入力があった段階でＳ１４９へ進み、その入力データを金融機関７のＶＰ管理サーバ９へ送信する処理がなされる。

【０２８０】

次にＳ１５０へ進み、本人証明処理が行なわれる。この本人証明処理は、ＶＰ出生依頼を行なったユーザが本人自身であるか否かを証明するための処理であり、図５４（ａ）にそのサブルーチンプログラムが示されている。ここで、図５４（ａ）に基づいて、その本人証明書のサブルーチンプログラムを説明する。

【０２８１】

この本人証明処理は、前述したＳ４，Ｓ６２等に基づいて乱数Ｒが送信されてきた場合にその乱数に基づいて本人証明を行なうためのものである。まずＳ１２５により、乱数Ｒを受信したか否かの判断がなされ、受信するまで待機する。乱数Ｒを受信した場合にはＳ２１６へ進み、その受信した乱数ＲをＩＣ端末１９Ｒまたは１９Ｖへ送信する処理がなされる。ＩＣ端末では、後述するように、記憶している認証鍵ＫＮまたは公開鍵ＫＰを用いて乱数Ｒを暗号化してレスポンスデータＩを生成して出力する処理が行われる。そのレスポンスデータＩが出力されてくれば、Ｓ２１７によりＹＥＳの判断がなされてＳ２１８へ進み、そのＩをＶＰ管理サーバ９へ送信する処理がなされる。

【０２８２】

図２９に示すＶＰ出生依頼処理を行なう場合には、ブラウザフォン３０のＵＳＢポート１８にＶＰ用ＩＣ端末１９Ｖを接続している。そして、ＶＰ出生依頼処理の際の本人証明処理では、ＶＰ用ＩＣ端末１９Ｖに記憶されているＲＰの認証鍵ＫＮを用いて乱数Ｒを暗号化する処理がなされる。これについては、後述する。

【０２８３】

その結果、図４９のＳ１５０のＶＰ出生依頼処理の際の本人証明では、ＲＰであることの証明がなされる。

【０２８４】

次にＳ１５１へ進み、アクセス拒絶を受信したか否かの判断がなされ、アクセス拒絶を受信した場合にＳ１５２へ進み、アクセス拒絶の表示が行なわれる。一方、アクセスが許容された場合にはＳ１５３へ進み、ＶＰ出生依頼を行なったユーザが希望するコンビニエンスストア２の入力があるか否かの判断がなされる。出生したＶＰの住所が、コンビニエンスストア２の住所となるために、ユーザは、自己の希望するコンビニエンスストア２がある場合には、そのコンビニエンスストア２を特定する情報をブラウザフォン３０のキー

ボードから入力する。入力があれば、Ｓ１５４により、その希望のコンビニエンスストア２のデータがＶＰ管理サーバ９へ送信される。希望のコンビニエンスストア２の入力がなかった場合には、前述したように、ＲＰの住所に最も近いコンビニエンスストア２の住所が出生したＶＰの住所となる。

【０２８５】

次にＳ１５５へ進み、ＶＰの公開鍵の送信要求があったか否かの判断がなされ、あるまで待機する。ＶＰ管理サーバ９では、前述したように、ＶＰの出生依頼があった場合に、ＶＰの公開鍵の送信要求を出す（Ｓ３０参照）。その送信要求をブラウザフォン３０が受ければ、制御がＳ１５６へ進み、ＶＰ用ＩＣ端末１９Ｖへ公開鍵出力要求を出す。すると、ＶＰ用ＩＣ端末１９Ｖが、記憶しているＶＰの公開鍵ＫＰを出力する。その出力があれば、制御がＳ１５８へ進み、その出力された公開鍵ＫＰを金融機関７のＶＰ管理サーバ９へ送信する。

【０２８６】

図５０（ｂ）は、Ｓ１０５に示された電子証明書発行要求処理のサブルーチンプログラムを示すフローチャートである。Ｓ１６５により、適正な暗証番号である旨のチェックが済んでいるか否かの判断がなされ、未だに済んでいない場合にはこのサブルーチンプログラムが終了する。一方、適正な暗証番号である旨のチェックが済んでいる場合にはＳ１６６へ進み、ＲＰ用電子証明書の発行依頼操作があったか否かの判断がなされる。ユーザがブラウザフォン３０のキーボードを操作して発行依頼を行なった場合には、制御がＳ１６７へ進み、ＲＰの住所，氏名の入力指示が表示される。ユーザがキーボードより入力すれば、制御がＳ１６９へ進み、ＲＰ用ＩＣ端末１９Ｒから公開鍵ＫＰを呼出す処理がなされる。この電子証明書発行要求処理を行なう場合には、ユーザは、ブラウザフォン３０のＵＳＢポート１８に自己のＲＰ用ＩＣ端末１９Ｒを接続しておく必要がある。そして、Ｓ１６９の処理が行なわれた場合には、その接続されているＲＰ用ＩＣ端末１９Ｒが記憶しているＲＰ用の公開鍵ＫＰがブラウザフォン３０に出力され、Ｓ１７０により、その出力されてきた公開鍵ＫＰと入力されたＲＰの住所，氏名とが金融機関７の認証用サーバ１１へ送信される。

【０２８７】

図５１（ａ）はＳ１０２に示されたＶＰ用入力処理のサブルーチンプログラムを示し、図５１（ｂ）はＳ１０６に示されたＲＰ用入力処理のサブルーチンプログラムを示すフローチャートである。

【０２８８】

ＶＰ用入力処理が行なわれる場合には、ブラウザフォン３０のＵＳＢポート１８にＶＰ用ＩＣ端末１９Ｖを接続しておく必要がある。Ｓ１７５により、適正な暗証番号である旨のチェックが終了しているか否かの判断がなされ、適正な暗証番号のチェックが未だなされていない場合にはこのサブルーチンプログラムが終了する。適正な暗証番号のチェック済の場合には、Ｓ１７６へ進み、ＶＰ用入力操作があったか否かの判断がなされる。前述したように、金融機関７のＶＰ管理サーバ９によりＶＰの出生処理が行なわれた場合には、誕生したＶＰの氏名，住所（コンビニエンスストア２の住所），コンビニエンスストア２の名称，Ｅメールアドレス，電子証明書が記憶されたＩＣ端末１９Ｉが郵送されてくるのであり、そのＩＣ端末１９Ｉをユーザがブラウザフォン３０に挿入すれば、Ｓ１７６によりＹＥＳの判断がなされてＳ１７８へ進み、そのＩＣ端末１９Ｉの記録データが読込まれて接続されているＶＰ用ＩＣ端末１９Ｖへ伝送される。

【０２８９】

ユーザがブラウザフォン３０のキーボードからＶＰ用ユーザエージェントの知識データの入力操作を行なえば、Ｓ１７７によりＹＥＳの判断がなされてＳ１７９へ進み、入力された知識データをＶＰ用ＩＣ端末１９Ｖへ伝送する処理がなされる。

【０２９０】

ユーザが金融機関７の自己の口座から資金を一部引落しすれば、その引落し額Ｇがブラウザフォン３０へ送信されてくる（Ｓ６９参照）。その引落し額Ｇがブラウザフォン３０

に入力されれば、Ｓ１８０によりＹＥＳの判断がなされてＳ１８１へ進み、引落し額ＧをＶＰ用ＩＣ端末１９Ｖへ転送してリロード金額として加算記憶させる処理がなされる。

【０２９１】

ＲＰ用入力処理が行なわれる場合には、ブラウザフォン３０のＵＳＢポート１８にＲＰ用ＩＣ端末１９Ｒを接続しておく必要がある。まずＳ１８５により、適正な暗証番号のチェックが済んでいるか否かの判断がなされ、済んでいる場合にはＳ１８６へ進み、ＲＰの電子証明書を受信したか否かの判断がなされる。ユーザがＲＰの電子証明書の発行依頼を認証用サーバに対し行なえば、前述したように、ＲＰの電子証明書が作なされてブラウザフォン３０に送信されてくる（Ｓ２８参照）。その電子証明書が送信されてくれば、Ｓ１８６によりＹＥＳの判断がなされてＳ１８７へ進み、受信した電子証明書をＲＰ用ＩＣ端末１９Ｒへ伝送して、ＲＰ用ＩＣ端末へ記憶させる処理がなされる。

【０２９２】

ユーザがブラウザフォン３０のキーボードを操作して、ＲＰ用ユーザエージェントの知識データの入力操作を行なえば、Ｓ１８８によりＹＥＳの判断がなされてＳ１８９へ進み、その入力された知識データをＲＰ用ＩＣ端末１９Ｒへ伝送する処理がなされ、ＲＰ用ＩＣ端末１９Ｒがその入力された知識データを記憶する。

【０２９３】

ユーザが決済サーバ１０に対し自己の口座内の資金の一部を引落す引落し要求を行なった場合には、前述したように、引落し金額であるＧが決済サーバ１０からユーザのブラウザフォン３０へ送信される。すると、Ｓ１９０によりＹＥＳの判断がなされてＳ１９１へ進み、引落し額ＧをＲＰ用ＩＣ端末１９Ｒへ伝送し、リロード金額としてＧを加算更新する処理が行なわれる。

【０２９４】

図５２は、ユーザ（ＲＰとＶＰが存在する）がクレジットカードの支払を行なってＳＥＴに従った決済が行なわれる場合の全体概略システムを示す図である。まず、カード会員がクレジットカードの発行手続を行なえば、クレジットカード発行会社４に設置されているサーバが、クレジット発行の申込みがあったことを判別して、当該カード会員に対しクレジットカード番号を発行する。その際に、カード会員がＶＰ用のクレジットカードの発行を要求した場合には、クレジットカード発行会社４のサーバは、そのＶＰの氏名や住所等のデータを入力してもらい、そのデータに基づいて金融機関などに登録されているＶＰか否かを金融機関７に問合せる。そして、金融機関７のデータベース１２に記憶されている正規のＶＰであることが確認されたことを条件として、クレジットカード発行会社４のサーバは、そのＶＰに対しクレジット番号を発行する処理を行なう。

【０２９５】

つまり、クレジットカード発行会社４のサーバは、仮想人物用のクレジット番号を発行するクレジット番号発行ステップを含んでいる。また、仮想人物用のクレジット番号を発行するクレジット番号発行手段を含んでいる。さらに、このクレジット番号発行ステップまたはクレジット番号発行手段は、前述したように、クレジット番号発行対象となる仮想人物が前記所定機関に登録されている正規の仮想人物であることが確認されたことを条件として、前記クレジット番号を発行する。クレジットカード発行会社４によって発行されたクレジットカード（ＲＰ用とＶＰ用の２種類存在する）を所持するユーザは、ＳＥＴによる取引をするための会員の登録要求を認証用サーバ１１に出す。認証用サーバ１１は、そのユーザがクレジットカード発行会社４のクレジット会員であるか否かの認証要求をクレジットカード発行会社４に出す。クレジットカード発行会社４からクレジットカードの会員である旨の認証の回答が認証用サーバ１１に返信されてくれば、認証用サーバ１１は、ＳＥＴ用の電子証明書を作成してカード会員に送る。

【０２９６】

電子モール等の加盟店６がＳＥＴによる取引を可能にするためには、まず、ＳＥＴによる取引のための会員登録要求を認証用サーバ１１に出す。認証用サーバ１１では、加盟店６が契約している加盟店契約会社（アクアイアラ）５に、当該加盟店６が正当な契約会社

であるか否かの認証要求を送信する。加盟店契約会社５から正当な加盟店である旨の回答が返信されてくれば、認証用サーバ１１は、その加盟店６のためのＳＥＴ用の電子証明書を作成して加盟店６に発行する。

【０２９７】

この状態で、カード会員が加盟店６により電子ショッピングを行なってＳＥＴにより取引を行なう場合には、まず商品やサービス等の購入要求をカード会員が加盟店６へ送信する。加盟店６では、その購入要求を承認してよいか否かの承認要求を支払承認部３３からペイメントゲートウェイ２７を介してクレジットカード発行会社４へ送信する。クレジットカード発行会社４から承認の回答がペイメントゲートウェイ２７を介して加盟店６に返信されてくれば、加盟店６は、購入を受理した旨をカード会員に送信する。また加盟店６は、支払要求部３４から支払要求をペイメントゲートウェイ２７に送信する。ペイメントゲートウェイ２７は、その支払要求に応じた決済要求をクレジットカード発行会社４へ送信するとともに、支払回答を加盟店６へ返信する。

【０２９８】

カード会員と加盟店６との間では、商品やサービスの購入取引を行なう際に、互いの電子証明書を送信して、正当な本人である旨の確認が行なわれる。

【０２９９】

クレジットカード発行会社４が、ユーザとしてのＲＰにクレジットカードを発行した場合には、そのクレジットカード番号等のカード情報が当該ユーザのＲＰ用ＩＣ端末１９Ｒに入力されて記憶される。一方、ユーザがＶＰとしてクレジットカード発行会社４からクレジットカードの発行を受ける際には、ＶＰ用に発行された電子証明書をクレジットカード発行会社４に送信し、金融機関７による身分の証明を行なってもらう必要がある。その上で、クレジットカード発行会社４がクレジットカードを発行した場合には、そのクレジットカードのカード番号等のカード情報が当該ユーザのＶＰ用ＩＣ端末１９Ｖに入力されて記憶される。

【０３００】

前述したＳＥＴ用の電子証明書の発行も、ＲＰ用とＶＰ用との２種類のケースに分けて発行される。そしてそれぞれ発行されたＳＥＴ用の電子証明書が、それぞれのＩＣ端末１９Ｒまたは１９Ｖに入力されて記憶される。

【０３０１】

図５３は、Ｓ１０３に示したＶＰ用決済処理のサブルーチンプログラムを示すフローチャートである。まずＳ１９５により、適正な暗証番号である旨のチェックが終了しているか否かの判断がなされ、終了していなければこのサブルーチンプログラムが終了し、適正な暗証番号のチェック済の場合にはＳ１９６へ進む。

【０３０２】

このＶＰ用決済処理は、金融機関７のユーザの銀行口座内の資金の一部を引落してＶＰ用ＩＣ端末１９Ｖへリロードする処理と、デビットカードを使用して決済を行なう処理と、クレジットカードを使用して決済を行なう処理と、ＶＰ用ＩＣ端末１９Ｖへリロードされているリロード金額を使用して決済を行なう場合とを有している。

【０３０３】

ユーザが自己の銀行口座内の資金を一部引落してＶＰ用ＩＣ端末へリロードする操作を行なえば、Ｓ１９７により、その引落し要求が金融機関７の決済サーバ１０へ送信される。次にＳ１９８へ進み、正当機関チェック処理（図３０Ａ参照）が行なわれる。

【０３０４】

次にＳ１９９へ進み、$R = D_{KP}(L)$である否かの判断がなされ、正当機関でない場合にはＳ１１９によりＮＯの判断がなされてＳ２００へ進み、正当機関でない旨の警告表示がなされる。一方、正当機関である場合には、$R = D_{KP}(L)$となるために、制御がＳ２０１へ進み、氏名の入力要求があったか否かの判断がなされ、あるまで待機する。前述したように、決済サーバ１０は、ＩＣ端末への引落し要求があった場合には、氏名の入力要求を送信する（Ｓ６０参照）。この氏名の入力要求が送信されてくれば、Ｓ２０１により

ＹＥＳの判断がなされてＳ２０２へ進み、ＶＰ用ＩＣ端末１９ＶからＶＰの氏名を呼出して決済サーバ１０へ送信する処理がなされる。次にＳ２０３へ進み、本人証明処理（図３４Ａ参照）がなされる。

【０３０５】

次にＳ２０４へ進み、引落し額の入力要求があったか否かの判断がなされ、なければＳ２０５へ進み、不適正な旨の返信があったか否かの判断がなされ、なければＳ２０４へ戻る。この２０４，２０５のループの巡回途中で、決済サーバ１０がユーザの正当性が確認できないと判断した場合には不適正である旨の返信を行なう（Ｓ７９参照）。その結果、Ｓ２０５によりＹＥＳの判断がなされてＳ２０７へ進み、不適正である旨がブラウザフォン３０のディスプレイにより表示される。一方、決済サーバ１０が本人認証の結果正当な本人であると判断した場合には引落し額の入力要求をブラウザフォン３０へ送信する（Ｓ８７参照）。すると、Ｓ２０４によりＹＥＳの判断がなされてＳ２０６へ進む。

【０３０６】

Ｓ２０６では、引落し額の入力指示をブラウザフォン３０のディスプレイに表示させる処理がなされる。ユーザがキーボードから引落し額を入力すれば、Ｓ２０８によりＹＥＳの判断がなされてＳ２０９へ進み、その入力された引落し額Ｇを決済サーバ１０へ送信する処理がなされる。決済サーバ１０では、引落し額Ｇを受信すれば、ＶＰの口座からＧを減算してＧを送信する処理がなされる（Ｓ８９参照）。その結果、Ｓ２１０によりＹＥＳの判断がなされてＳ２１１へ進み、引落し額ＧをＶＰ用ＩＣ端末１９Ｖへ送信してＧをリロード金額に加算更新する処理がなされる。

【０３０７】

Ｓ１９６により、ＮＯの判断がなされた場合には、図５４（ｂ）のＳ２２０へ進み、デビットカードの使用操作があったか否かの判断がなされる。デビットカードの使用操作があった場合には、Ｓ２３５へ進み、デビットカード使用要求を決済サーバ１０へ送信する処理がなされる。次にＳ２２１へ進み、正当機関チェック処理（図５０（ａ）参照）がなされる。そしてＳ２２２へ進み、$R = D_{KP}(L)$であるか否かの判断がなされる。正当機関でない場合には、ＮＯの判断がなされてＳ２２３へ進み、正当機関でない旨の警告表示がなされる。一方、正当機関である場合には制御がＳ２２４へ進み、デビットカードの暗証番号とカード情報の入力要求があったか否かの判断がなされ、あるまで待機する。決済サーバ１０は、デビットカードの使用要求があった場合には、暗証番号とカード情報の入力要求をブラウザフォン３０へ送信する（Ｓ７０参照）。その送信を受信すれば、制御がＳ２２５へ進み、暗証番号の入力指示がブラウザフォン３０の表示部７６に表示される。ユーザがデビットカードの暗証番号をキーボードから入力すれば、Ｓ２２６によりＹＥＳの判断がなされてＳ２２７へ進み、ＶＰ用ＩＣカード１９Ｖからカード情報を読出し暗証番号とともに決済サーバ１０へ送信する処理がなされる。

【０３０８】

次にＳ２２８へ進み、不適正である旨の返信があったか否かの判断がなされる。暗証番号とカード情報とを受信した決済サーバ１０は、適正か否かの判断を行ない（Ｓ７２）、適正でない場合には不適正である旨の返信を行なう（Ｓ７９参照）。不適正である旨が返信されてくれば、Ｓ２２８によりＹＥＳの判断がなされてＳ２２９へ進み、不適正である旨の表示がなされる。一方、不適正である旨の返信が送られてこなければ、制御がＳ２３０へ進み、使用金額の入力指示がパーソナルコンピュータのディスプレイに表示される。ユーザが使用金額をキーボードから入力すれば、Ｓ２３１によりＹＥＳの判断がなされてＳ２３２へ進み、入力された使用金額Ｇを決済サーバ１０へ送信する処理がなされる。

【０３０９】

使用金額Ｇを受信した決済サーバ１０は、前述したように、ユーザに該当する銀行口座を検索して使用金額Ｇを減算するとともに、その使用金額Ｇをブラウザフォン３０に返信する処理を行なう（Ｓ７４）。

【０３１０】

その結果、Ｓ２３３によりＹＥＳの判断がなされてＳ２３４へ進み、決済が完了した旨

の表示をブラウザフォン３０の表示部７６に表示させる処理がなされる。

【０３１１】

Ｓ２２０によりＮＯの判断がなされた場合には、制御がＳ２３８へ進む。Ｓ２３８では、クレジットカードの使用操作があったか否かの判断がなされる。ユーザがブラウザフォン３０のキーボード７７を操作してクレジットカードの使用を入力すれば、制御がＳ２３７へ進み、クレジットカードによる決済要求を加盟店６へ送信する処理がなされる。この加盟店は、ユーザが商品やサービスを購入しようとしている商店である。次に制御がＳ２３９へ進み、正当機関チェック処理がなされる。この正当機関チェック処理は、図５０（ａ）に示したものである。この正当機関チェック処理に合せて、加盟店６は、当該加盟店の電子証明書を顧客のブラウザフォン３０へ送信し、次に乱数Ｒを受信すれば、その乱数を自己の秘密鍵ＫＳを用いて暗号化し、その暗号結果Ｌを顧客のブラウザフォン３０へ送信する。

【０３１２】

制御がＳ２４０へ進み、$R = D_{KP}(L)$であるか否かの判断がなされる。正当な販売店（加盟店）でない場合には、Ｓ２４０によりＮＯの判断がなされて、Ｓ２４１へ進み、正当な販売店でない旨の警告表示がなされる。一方、正当な販売店（加盟店）である場合には、Ｓ２４２へ進み、オーダ情報ＯＩと支払指示ＰＩとが作なされる。オーダ情報ＯＩとは、商品やサービス等の購入対象物や購入個数等を特定するための情報である。支払指示ＰＩは、たとえばクレジット番号何々のクレジットカードを利用してクレジットの支払を行なう旨の指示等である。

【０３１３】

次にＳ２４３へ進み、オーダ情報ＯＩと支払指示ＰＩのメッセージダイジェストを連結した二重ダイジェストＭＤを算出する処理がなされる。次にＳ２４４へ進み、二重ダイジェストＭＤとクレジットカードを使用するＶＰ氏名とをＶＰ用ＩＣ端末１９Ｖへ伝送して署名指示を出すとともに、ＶＰ用電子証明書の出力要求を行なう。

【０３１４】

クレジットカードを使用するＶＰ氏名と署名指示と電子証明書の出力要求を受けたＶＰ用ＩＣ端末１９Ｖは、入力されたＶＰ氏名をトラップ型ＲＦＩＤ記憶領域と照合してそのＶＰ氏名がＶＰの本名Ｂ１３Ｐ（図９参照）を何回暗号化したものかを割出す。そしてその回数だけ秘密鍵を秘密鍵で暗号化して、その暗号化秘密鍵（ＫＳ）を用いて入力されたＭＤを復号化していわゆる二重署名を生成する。この二重署名を便宜上$D_{(KS)}$（ＭＤ）と表現する。ＶＰ用ＩＣ端末１９Ｖは、その$D_{(KS)}$（ＭＤ）をブラウザフォン３０へ出力する。

【０３１５】

Ｓ２４４に従って入力されたＶＰ氏名がＶＰの本名Ｂ１３Ｐであった場合には、ＶＰ用ＩＣ端末１９Ｖは、その本名に対する電子証明書を格納しているために、その格納している電子証明書をブラウザフォン３０へ出力する。一方、Ｓ２４４に従って入力されたＶＰ氏名がトラップ型ＶＰ氏名であった場合には、ＶＰ用ＩＣ端末１９Ｖがそのトラップ型ＶＰ氏名用の電子証明書を格納していない。そのトラップ型ＶＰ氏名用の電子証明書は、前述したようにＸＭＬストア５０に格納されている。よって、その場合には、ＶＰ用ＩＣ端末１９Ｖは、ＸＭＬストア５０に電子証明書を取寄せる旨の指示をブラウザフォン３０へ出力する。

【０３１６】

Ｓ２４４の要求をＶＰ用ＩＣ端末１９Ｖへ出力した後、ＶＰ用ＩＣ端末１９Ｖから何らかの返信があれば、Ｓ２４５によりＹＥＳの判断がなされてＳ６０５へ制御が進む。Ｓ６０５では、ＸＭＬストア５０への電子証明書の取り寄せ指示であったか否かの判断がなされ、取り寄せ指示でなかった場合にはＳ２４６へ進むが、取り寄せ指示であった場合には制御がＳ６０６へ進む。Ｓ６０６では、ＸＭＬストア５０へアクセスしてトラップ型ＶＰ氏名に対応する電子証明書を検索してＳ２４６へ進み、オーダ情報ＯＩと支払指示ＰＩと出力されてきた署名としての$D_{(KS)}$（ＭＤ）とＶＰ用電子証明書とを加盟店６へ送信する

処理がなされる。加盟店６では、それら情報を確認した上で、ユーザの購入要求を受理する購入受理の回答をユーザのブラウザフォン３０へ送信する。すると、Ｓ２４７によりＹＥＳの判断がなされてＳ２４８へ進み、取引が完了した旨の表示が行なわれる。

【０３１７】

Ｓ２３８によりＮＯの判断がなされた場合にＳ２４９へ進み、リロード金額の使用操作があったか否かの判断がなされる。ユーザが、ＶＰ用ＩＣ端末１９Ｖに蓄えられているリロード金額を使用する旨のキーボード操作を行なえば、制御がＳ２５０へ進み、使用金額の入力指示がブラウザフォン３０のディスプレイに表示される。ユーザが使用金額をキーボードから入力すれば、Ｓ２５１によりＹＥＳの判断がなされてＳ２５２へ進み、入力された使用金額Ｇの引落し要求をＶＰ用ＩＣ端末１９Ｖへ伝送する処理がなされる。

【０３１８】

ＶＰ用ＩＣ端末１９Ｖでは、後述するように、引落し要求を受ければ、その使用金額Ｇだけリロード金額を減算更新し、引落しが完了した旨の信号をブラウザフォン３０へ返信する。すると、Ｓ２５２ａによりＹＥＳの判断がなされてＳ２５２ｂへ進み、Ｇの支払処理がなされる。

【０３１９】

なお、ＲＰ用決済処理は、以上説明したＶＰ用決済処理とほとんど同じ内容の処理であるために、図示および説明の繰返しを省略する。

【０３２０】

図５６は、図２７に示したＲＦＩＤ交換処理の他の例のサブルーチンプログラムを示すフローチャートである。図５６のＲＦＩＤ交換処理では、ブラウザフォン３０により通話を行うことによりＲＦＩＤの交換を行う。図２７と同じ処理を行うスッテップには同じステップ番号を付してあり、ここでは主に相違点について説明する。ＳＳ１により、ブラウザフォン３０により通話を行ったか否かの判断がなされる。通話を行った場合にはＳＥ３に進み、今日既に交換済みの相手（ブラウザフォン３０）でないことを条件にＳＥ４以降のＲＦＩＤ交換処理を行う。

【０３２１】

図５７は、図２７に示したＲＦＩＤ交換処理のさらに他の例のサブルーチンプログラムを示すフローチャートである。図５７のＲＦＩＤ交換処理では、ブラウザフォン３０により電子メールの送受信を行うことによりＲＦＩＤの交換を行う。ＳＴ１によりＥメール（電子メール）の送信を行ったか否かの判断がなされる。行っていないば場合には、ＳＴ２へ進み、Ｅメールを受信したか否かの判断がなされる。受信していない場合には、このサブルーチンプログラムが終了する。

【０３２２】

Ｅメールを送信する場合には、ＳＴ１よりＹＥＳの判断がなされ、ＳＥ３により、今日既にＲＦＩＤを交換済みの相手（ブラウザフォン３０）か否かの判断がなされる。既に交換済みの相手の場合には、このサブルーチンプログラムが終了する。交換済みでない場合には、ＳＥ４へ進み、偽ＲＦＩＤを記憶しているか否かの判断がなされる。ブラウザフォン３０のＥＥＰＲＯＭ１９４に偽ＲＦＩＤを記憶しておれば、制御がＳＴ３へ進み、その記憶している偽ＲＦＩＤをＥメールとともに相手のブラウザフォン３０に発信する。一方、ＥＥＰＲＯＭ１９４に偽ＲＦＩＤを全く記憶していない場合には、ＳＥ５以降の偽ＲＦＩＤを生成して相手に送信する処理がなされる。

【０３２３】

Ｅメールを受信した場合には、ＳＴ８へ進み、Ｅメールの相手から送られてきた偽ＲＦＩＤを受信する。次にＳＥ９へ進み、ＥＥＰＲＯＭ１９４に既に記憶している偽ＲＦＩＤを１つずつ古い記憶エリア側にシフトし、記憶上限を超えた１番古い偽ＲＦＩＤを消去する処理がなされる。次にＳＥ１０へ進み、１番新しい記憶エリアに受信した偽ＲＦＩＤを記憶する処理がなされる。

【０３２４】

なお、図５６、図５７に示したＲＦＩＤ交換処理を、図２６に示したＲＦＩＤ交換処理

の代わりに用いるのではなく、図２６に示したＲＦＩＤ交換処理にさらに付け加えて用いるようにしてもよい。また、個人ユーザがブラウザフォン３０を操作して、図２６、図５６、図５７のＲＦＩＤ交換処理の内の任意の１つまたは２つ以上のものを適宜選択して使用できるようにしてもよい。

【０３２５】

ユーザがアクセスし自己の個人情報を提供した業者を特定するために用いる識別情報を特定可能な情報であって、前記個人情報を入手した者がその個人情報主であるユーザにメール（Ｅメールやダイレクトメール）を送る場合には該メールに含まれることとなる識別情報として、前述した実施の形態では匿名（トラップ型ＶＰ氏名）を用いたが、その代わりにまたはそれに加えて、業者毎に使い分ける複数のＥメールアドレスやダイレクトメール用の住所(コンビニエンスストアの住所または私書箱等)を用いてもよい。すなわち、次のような個人情報保護装置であればよい。

【０３２６】

コンピュータシステムを利用して、個人情報を保護する個人情報保護装置であって、ユーザが自己の個人情報を提供した業社を特定するために用いる識別情報を特定可能な情報であって、前記個人情報を入手した者がその個人情報主であるユーザにメール（Ｅメール、ダイレクトメール）を送る場合には該メールに含まれることとなる識別情報を特定可能な情報（匿名としてのトラップ型ＶＰ氏名,図４４（ａ）のＫＳＢとサイト名,サイト毎に使い分けるＥメールアドレスやダイレクトメール用の住所）を格納する識別情報格納手段（データベース１２ａ，ＥＥＰＲＯＭ２６）と、前記個人情報を入手した者がその個人情報主であるユーザに対し送ったメール（Ｅメール，ダイレクトメール）に含まれている前記識別情報に基づいて特定される前記業社と前記メールの送り主とが一致するか否かを判定して前記ユーザの個人情報の流通状態を監視する監視手段（Ｓ５１６，Ｓ５２２，Ｓ５２３）とを含む個人情報保護装置。

【０３２７】

前述の実施の形態では、トラップ型ＶＰを利用しての個人情報の不正漏洩者と漏洩した個人情報の不正入手者との割出しを、トラップ型ＶＰの氏名を手掛かりに行なうものを示した。そして、別実施の形態において、トラップ型ＶＰのＥメールアドレスをトラップ型ＶＰ毎に異ならせてもよい旨を示した。この別実施の形態のように、トラップ型ＶＰの氏名の代わりにトラップ型ＶＰのＥメールアドレスを利用し、前述の個人情報不正流出者と漏洩した個人情報の不正入手者とを割出すようにしてもよい。即ち、トラップ型ＶＰ毎に異なるＥメールアドレスを登録しておき、トラップ型ＶＰ宛にＥメールが送信されて来た場合に、そのＥメールの送信先であるＥメールアドレスと一致するトラップ型ＶＰのＥメールアドレスを割出し、その割出されたＥメールアドレスに対応する業社（トラップ型ＶＰのＥメールアドレスを通知した業社）を割出し、その割出された業社とＥメールを送信してきた送信元とが一致するか否かの整合性チェックを行ない、一致しない場合には前述のＳ５１９～Ｓ５２１の異常時処理を行なう。

【０３２８】

なお、このようなＥメールアドレスの基づいた整合性チェックを行う場合には、トラップ型ＶＰに限定して行う必要がなく、ＲＰが行うようにしてもよい。即ち、ＲＰが自己の複数のＥメールアドレスを所有し、サイト（業社）毎に異なるＥメールアドレスを通知すると共にどのＥメールアドレスをどの業社に通知したかをＶＰ管理サーバ９または後述するメールサーバ８０に登録しておき、送信されてきたＥメールの送信先のＥメールアドレスからそのＥメールアドレスを通知した業社（サイト）を割出し、その割出された業社とＥメールの送信元とが一致するか否かの整合性チェックを行ない、個人情報の不正漏洩者や不正入手者を割出すようにしてもよい。

【０３２９】

以下に、Ｅメールアドレスを利用した整合性チェックによる個人情報の不正流出者（不正漏洩者）と不正入手者との割出しを行う監視システムを説明する。

【０３３０】

図５８は、メールサーバ８０およびそのデータベース８１に記憶されているデータを示す図である。このメールサーバ８０は、図１の広域・大容量中継網４３やインターネット１や携帯電話網５４等に接続されているものであり、ブラウザフォン３０等のメールクライアントから送信されたＥメールをその発信先Ｅメールアドレスに対応する送信先のメールボックスにまで送信して格納するためのものである。図５８に示すように、データベース８１には、鍵指定番号、共通鍵（ＫＮ）、Ｅメールアドレスの各データが記憶されているとともに、Ｅメールアドレスに対応するメールボックスが設けられている。共通鍵（ＫＮ）は、前述した認証鍵ＫＮのことであるが、認証鍵ＫＮに限らず、個人ユーザ（ＲＰとＶＰの両者を含む）がメールサーバ８０へ登録した共通鍵暗号方式用のＥメール専用の鍵であってもよい。

【０３３１】

鍵指定番号は、そのメールサーバ８０に登録されている共通鍵を指定するための番号である。この番号に従って登録されている複数の共通鍵のうちの対応する共通鍵が検索される。そのＥメールアドレスは、メールサーバ８０に登録されているユーザのＥメールアドレスである。尚、あるユーザが複数のＥメールアドレスをメールサーバ８０に登録する場合もあり、その場合には、例えば、一つの鍵指定番号によってそのユーザの一つの共通鍵が特定されれば、その一つの共通鍵に対応するＥメールアドレスが複数存在することとなる。

【０３３２】

図５９は、ブラウザフォン３０によって行われるＥメールアドレス通知処理のサブルーチンプログラムを示すフローチャートである。図５９（ｂ）は、ＩＣ端末１９Ｒまたは１９Ｖにより行われるＥメールアドレス生成処理のサブルーチンプログラムを示すフローチャートである。

【０３３３】

図５９（ａ）を参照して、ＳＵ１により、Ｅメールアドレス生成操作があったか否かの判断がなされ、ない場合にはこのサブルーチンプログラムが終了する。個人ユーザがブラウザフォン３０を操作してＥメールアドレス生成操作を行えば、ＳＵ１によりＹＥＳの判断がなされてＳＵ２へ進み、Ｅメールアドレスを通知する相手を特定する情報である通知相手特定情報を入力するメッセージ表示をブラウザフォン３０により行う制御がなされる。この通知相手特定情報は、後述するように、通知相手の業社名と通知相手のＥメールアドレスである。次にＳＵ３により、通知相手特定情報の入力があったか否かの判断がなされ、あるまで待機する。個人ユーザがブラウザフォン３０を操作して通知相手特定情報（通知相手の業社名と通知相手のＥメールアドレス）を入力すれば、ＳＵ４へ進み、通知相手特定情報をブラウザフォン３０に接続されているＩＣ端末（１９Ｒ又は１９Ｖ）に入力する制御がなされる。

【０３３４】

次にＳＵ５により、接続されているＩＣ端末から通知用Ｅメールアドレスが出力されて来たか否か判断され、出力されてくるまで待機する。出力されて来れば、ＳＵ６へ進み、その出力されて来た通知用Ｅメールアドレスをブラウザフォン３０により表示させる制御を行う。そしてＳＵ６ａにより、その表示された通知用Ｅメールアドレスを通知相手に送信するための操作が行われたか否かの判断がなされる。通知用Ｅメールアドレスを通知する相手に対し、インターネットあるいはブルートゥース等の無線を使用して通知する場合には、その旨の操作をブラウザフォン３０により行う。すると、制御がＳＵ７へ進み、その通知用Ｅメールアドレスが通知相手に送信されることとなる。

【０３３５】

図５９（ｂ）参照して、Ｓ１０００により、通知相手特定情報がブラウザフォン３０から入力されたか否かの判断がなされ、入力されていない場合には、このサブルーチンプログラムが終了する。入力された場合にはＳ１００１へ進み、その入力された通知相手特定情報と個人ユーザのＥメールアドレスとの両者を含むデータを共通鍵ＫＮで暗号化する処理を行う。そしてＳ１００２へ進み、その暗号結果のデータ中に鍵指定番号を分散挿入し

て通知用のＥメールアドレスを生成する。そしてＳ１０３により、その生成された通知用のＥメールアドレスをブラウザフォン３０へ出力する処理を行う

ブラウザフォン３０では、Ｓ１００３により通知用Ｅメールアドレスが出力されて来れば、前述したようにＳＵ５によりＹＥＳの判断がなされてＳＵ１６以降の処理を実行する

図６０は、メールサーバ８０の制御動作を示すフローチャートである。ＳＶ１によりＥメールアドレスの登録要求があったか否かの判断がなされる。ない場合にはＳＶ２へ進み、Ｅメールを受信したか否かの判断がなされ、受信していない場合にはＳＶ３へ進み、その他の処理を行ってＳＶ１へ戻る。このＳＶ１→ＳＶ３をループの巡回途中で、ユーザからＥメールアドレスの登録要求があった場合には、制御がＳＶ４へ進み、そのユーザから送信されてきたＥメールアドレスをデータベース８０に登録する処理が行われる。その際に、当該ユーザの共通鍵やその共通鍵を指定するための鍵指定番号がデータベース８０に未だ登録されていない場合には、メールサーバ８０は、当該ユーザのための共通鍵とそれに対応する鍵指定番号とを生成してデータベース８１に登録する。

【０３３６】

次に、Ｅメールを受信すれば、ＳＶ２によりＹＥＳの判断がなされてＳＶ５へ進み、その受信したＥメールのＥメールアドレス（ＳＵ７により送信した通知用Ｅメールアドレス）から鍵指定番号を抽出する処理が行われる。前述したように、通知用Ｅメールアドレスには、ユーザの鍵指定番号が分散挿入されており（Ｓ１００２参照）、その分散挿入されている鍵指定番号をこのＳＶ５により抽出するのである。次に制御がＳＶ６に進み、その抽出された鍵指定番号に対応する共通鍵ＫＮをデータベース８１を検索して割出し、ＳＶ７により、受信した通知用Ｅメールアドレスから鍵指定番号を抽出した残りのデータをＤＰとしてそのＤＰをＳＶ６により検索した共通鍵ＫＮにより復号する演算を行なう。

【０３３７】

次に、ＳＶ８により、メールヘッダ部分を読込み、ＳＶ９によりその読込んだメールヘッダ部分を解析し、ＳＶ１０により受信Ｅメールの送信元の氏名とＥメールアドレスとを抽出する。

【０３３８】

次に、ＳＶ７による演算結果データの中の通知相手特定情報により特定される通知相手の業社名およびＥメールアドレスとＳＶ１０により抽出された送信元（差出人）の氏名およびＥメールアドレスとが一致するか否かを、Ｓ１１によりチェックする処理が行われる。この一致判別は、受信したＥメールに送信元（差出人）の氏名が示されておらず送信元（差出人）のＥメールアドレスしか示されていなかった場合には、そのＥメールアドレスとＳＶ７による演算結果のデータ中の通知相手特定情報により特定されるＥメールアドレスとが一致するか否かのみにより判断する。ＳＶ１１によるチェックの結果、一致するか否かがＳＶ１２により判断され、一致する場合にはＳＶ１３に進み、演算結果データ中のＥメールアドレスに相当するメールボックス（図５８参照）に受信したＥメールを格納する処理が行われる。

【０３３９】

一方、ＳＶ１１により、一致しないか判断された場合には、ＳＶ１４へ進み、Ｅメールの受信元（差出人）に対応させて個人情報の不正入手値を「１」加算更新し、ＳＶ１５により、特定された通知相手に対応させて個人情報の不正流出者の不正流出値を「１」加算更新し、ＳＶ１６により演算結果データ中のＥメールアドレスに相当するメールボックスに個人情報の漏洩レポートを格納する処理が行われる。個人ユーザは、自己のメールボックス中に格納された個人情報の漏洩レポートを呼出すことにより、個人情報の不正入手者、個人情報の不正流出者、送信されてきたＥメールの内容等の詳しいレポートを閲覧することが出来る。また、メールサーバ８０は、ＳＶ１４、ＳＶ１５の集計結果を公表する。なお、ＳＶ１６の処理の代わりにまたはＳＶ１６の処理に加えて、個人情報の漏洩レポートを前述の個人情報の不正流出者宛さらには所定の個人情報保護機関（警察庁の担当部署等）に送信してもよい。

【０３４０】

さらに、前述のＳＧ１３により予め選択指定されている業者に対応するＲＦＩＤを発信した場合に、その予め選択指定されている業者名とＲＦＩＤを発信した発信先の業者名とを対応付けてブラウザフォン３０等に記憶しておくとともに、メールサーバ８０等にも予め選択指定されている業者名とＲＦＩＤを発信した発信先の業者名とを送信して、両者を対応付けて記憶させるようにしてもよい。このようにすれば、個人情報の不正入手者と個人情報の不正流出者が、予め選択指定されている業者名とＲＦＩＤを発信した発信先の業者名の記憶情報に一致したときには、前述の個人情報の不正入手者がＳＧ１３により発信されたトラップ型ＲＦＩＤを悪用して個人情報を不正に入手した者である疑いが高くなる。

【０３４１】

図６１は、図５９、図６０に示した制御内容を分かり易く説明するための説明図である。先ず、個人ユーザが顧客またはユーザとして業社に自己のＥメールアドレスを通知する際には、個人ユーザ側端末としてのブラウザフォン３０にＩＣ端末１９を取付けて通知用のＥメールアドレスを生成する。ＩＣ端末１９は、個人ユーザがＶＰとしてＥメールアドレスを通知する場合にはＶＰ用ＩＣ端末１９Ｖを用い、個人ユーザがＲＰとしてＥメールアドレスを通知する場合にはＲＰ用ＩＣ端末１９Ｒを用いる。通知用Ｅメールアドレスを生成するには、先ず、業社側端末８２から通知相手の業社の業社名ＭＴＴとＥメールアドレス○△××△とからなる通知相手特定情報ＭＴＴ//○△××△を送信してもらう。その通知相手特定情報を受信したブラウザフォン３０およびＩＣ端末１９において、前述したように、受信した通知相手特定情報（ＭＴＴ//○△××△）と個人ユーザ（ＶＰまたはＲＰ）のＥメールアドレス（○□×△×）とを個人ユーザの共通鍵ＫＮＩにより暗号化、すなわちE_{KNI}（ＭＴＴ//○△××△//○□×△×）を演算して、＃ｅ¥８％３＆αｔ＊ｃを生成する。この暗号データに予め決められたフォーマットに従って鍵指定番号（９２１０３）を分散挿入する。この実施の形態の場合、左から数えて、２番目と３番目の間、４番目と５番目の間、６番目と７番目の間、７番目と８番目の間、８番目と９番目の間に、鍵指定番号（９２１０３）の各数値を１つずつ分散挿入する。そして出来上がった＃ｅ９¥８２％３１＆０α３ｔ＊ｃを、通知用Ｅメールアドレスとして業社側端末８２へ送信する。

【０３４２】

以降、業社側は、＃ｅ９¥８２％３１＆０α３ｔ＊ｃをＥメールアドレスとして個人ユーザにＥメールを送ることとなる。業社ＭＴＴが業社側端末８２によりＥメール８５を作成し、送信先Ｅメールアドレスを＃ｅ９¥８２％３１＆０α３ｔ＊ｃとしてＥメール８５を送信すれば、そのＥメール８５がメールサーバ８０に送られる。メールサーバ８０では、前述の鍵指定番号の挿入フォーマットに従って、Ｅメール８５の送信先Ｅメールアドレス＃ｅ９¥８２％３１＆０α３ｔ＊ｃ中に分散挿入されている鍵指定番号を抽出する。その抽出した鍵指定番号９２１０３に基づいてデータベース８１を検索して対応する鍵ＫＮＩを割出す。次に、送信先Ｅメールアドレスから鍵指定番号を抜き去った残りのデータ＃ｅ¥８％３＆αｔ＊ｃを前述の割出された共通鍵ＫＮＩで復号する演算、すなわちD_{KNI}（＃ｅ¥８％３＆αｔ＊ｃ）を行ない、ＭＴＴ//○△××△//○□×△×を算出する。この算出データ中のＭＴＴ//○△××△が通知相手特定情報であり、本来なら、受信Ｅメール８５の送信元の名前とＥメールアドレスに一致するはずである。この通知相手特定情報であるＭＴＴ//○△××△と受信Ｅメール８５の送信元の名前およびＥメールアドレスとを比較し、一致しておれば、算出したＭＴＴ//○△××△//○□×△×中の送信先Ｅメールアドレスである○□×△×に相当するメールボックスに受信Ｅメールを格納する。その結果個人ユーザが自分のメールボックスにアクセスして受信Ｅメールをダウンロードして閲覧可能となる。

【０３４３】

一方、通知相手特定情報であるＭＴＴ//○△××△と受信Ｅメール８５の送信元の名前およびＥメールアドレスとを比較し、一致していなければ（たとえば、送信元の名前がＭＥＣ等の場合）、通知相手業者ＭＴＴから個人ユーザのＥメールアドレスを含む個人情報

が漏洩され、その漏洩されたＥメールアドレスを不正入手した者（たとえば、ＭＥＣ）がそのＥメールアドレス宛にＥメールを送信してきたことが想定されるため、前述のＳＶ１４～ＳＶ１６の異常時処理を行なう。

【０３４４】

以上の監視システムでは、個人情報の不正入手者（たとえば、ＭＥＣ）が自己の業社名やＥメールアドレスを使用することな個人情報の不正流出者の業社名（たとえば、ＭＴＴ）やＥメールアドレスを使用してＥメールを送信した場合には、不正の監視ができない。しかし、個人情報の不正入手者（たとえば、ＭＥＣ）は、たとえば自社製品の売込みや宣伝等の営業活動の一環としてＥメールを送信するのであり、Ｅメールの送信元として他社の業社名（たとえば、ＭＴＴ）やＥメールアドレスを使用したのでは、自社製品の売込みや宣伝等の営業活動にはならない。よって、個人情報の不正入手者の営業活動としてのＥメールの送信に対しては、有効な監視システムである。

【０３４５】

なお、前述の通知相手特定情報であるＭＴＴ//○△××△と受信Ｅメール８５の送信元の名前およびＥメールアドレスとの比較判定は、完全に一致するか否かにより判定してもよいが、少なくともＥメールアドレスが一致していれば適正と判定してもよい。また、受信Ｅメールに含まれている送信元特定情報として、送信者名と送信元Ｅメールアドレスとのいずれか一方しかない場合がある。その場合は、そのずれか一方の送信元特定情報と通知相手特定情報とが一致すれば適正であると判定してもよい。さらに、通知相手特定情報を通知相手のＥメールアドレスのみにしてもよい。

【０３４６】

以上説明したＥメールアドレスを利用した整合性チェックによる個人情報の不正流出者（不正漏洩者）と不正入手者との割出しを行なう監視システムは、Ｅメールの受取り側のみが暗号化Ｅメールアドレスを採用している場合を示した。次に、Ｅメールの受取り側と送信側との双方が暗号化Ｅメールアドレスを採用している場合を説明する。先ず、双方が互いのＥメールアドレス○□×△×、○△××△を送信し、受信した相手のＥメールアドレスを用いて前述と同様の方法で通知用Ｅメールアドレスを生成して相手に返信して通知する。業者ＭＴＴが個人ユーザにＥメールを送るときには、前述と同様に、送信先Ｅメールアドレスとして＃ｅ９¥８２％３１＆０αｓｔ＊ｃ、送信元の名前としてＭＴＴ、送信元Ｅメールアドレスとして○△××△のＥメール８５を作成して送信する。メールサーバ８０での整合性チェックも前述と同様の方法で行なう。

【０３４７】

なお、Ｅメール８５を受信した個人ユーザがＥメールを返信するときには、Ｅメール８５に示されている送信元のＥメールアドレス○△××△に返信したのでは業者ＭＴＴに届かない。業者ＭＴＴから通知してもらった通知用Ｅメールアドレス、すなわち個人ユーザ名と個人ユーザのＥメールアドレス○□×△×とを業者の共通鍵（たとえばＫＮ１）で暗号化したデータに鍵指定番号を分散挿入して生成された通知用Ｅメールアドレス宛に、Ｅメールを返信しなければならない。これを可能にするため、個人ユーザのブラウザフォン３０は、業者ＭＴＴから通知された通知用Ｅメールアドレスと業者ＭＴＴのＥメールアドレス○△××△とを対応付けて記憶しており、Ｅメールアドレス○△××△を入力することによって業者ＭＴＴの通知用Ｅメールアドレスを検索して出力できるように構成されている。業者ＭＴＴの端末８２も同様に、個人ユーザから通知された通知用Ｅメールアドレスと個人ユーザのＥメールアドレス○□×△×とを対応付けて記憶しており、Ｅメールアドレス○□×△×を入力することによって個人ユーザの通知用Ｅメールアドレスを検索して出力できるように構成されている。

【０３４８】

このような、送信されてきたＥメールの送信元Ｅメールアドレスをそのまま使用してＥメールの返信ができない不都合を解消する方法として、次のような変形システムを採用してもよい。互いにＥメールアドレスを交換して相手のＥメールアドレスを用いて通知用Ｅメールアドレスを生成して返信し、Ｅメール８５を相手の通知用Ｅメールアドレス宛に送

信する点は、前述と同じであるが、Ｅメール８５の送信元のＥメールアドレスを相手に通知した送信元の通知用Ｅメールアドレスにする。これにより、Ｅメール８５を受信した者は、そのＥメール８５に示されている送信元の通知用Ｅメールアドレス宛にそのままＥメールを返信すれば、そのＥメールが送信元に届く。そして、メールサーバ８０において、送信されてきたＥメール８５の送信先Ｅメールアドレス#ｅ９¥８２%３１＆０αｔ＊ｃから算出された通知相手特定情報中のＥメールアドレス○△××△とＥメール８５に示されているの送信元の通知用Ｅメールアドレスとを直接比較するのではなく、通知用Ｅメールアドレスを前述の演算手順に従って復号してＥメールアドレス○△××△を算出し、その算出されたＥメールアドレスと送信先Ｅメールアドレスから算出された通知相手特定情報中のＥメールアドレスとを比較判定する。

【０３４９】

また、通知用Ｅメールアドレス（たとえば#ｅ９¥８２%３１＆０αｔ＊ｃ）を、通常のＥメールアドレス（たとえば○□×△×）に比べて一見区別がつかない記号の組合せで構成するようにしてもよい。これにより、個人情報の不正入手者が、不正入手した個人情報中の通知用Ｅメールアドレスを通常のＥメールアドレスと思い、なんら疑うことなく通知用Ｅメールアドレス宛にＥメールを送信することとなり、罠にかかり易くなる利点がある。

【０３５０】

さらに、暗号化して通知用Ｅメールアドレスを生成するのに代えて、通知相手毎に専用のＥメールアドレスを生成して、該専用Ｅメールアドレスとそれに対応する通知相手とを対応付けてメールサーバ８０およびブラウザフォン３０等に登録しておくようにしてもよい。そして、送信されてきたＥメールの送信先Ｅメールアドレスである専用Ｅメールアドレスに対応する通知相手を登録されている通知相手から検索して割出し、その割出された通知相手と送信されて来たＥメールの送信元とが一致するか否かの整合性チェックを行う。なお、この発明における「暗号化」とは、所定のアルゴリズムに従ってデータを変換するのも全てを含む広い概念である。また、「復号」とは、暗号化されたデータを所定のアルゴリズムに従って元のデータに戻すもの全てを含む広い概念である。

【０３５１】

以上説明した、個人情報の不正流出者（不正漏洩者）と不正入手者との割出しを行なう監視システムは、自己のメールアドレス（通知用Ｅメールアドレス）を自ら通知した相手以外の者からのＥメールの受信を防止でき、迷惑メール（スパム）を有効に防止できる利点も有している。また、個人ユーザと業者との間でＥメールを送受信するものを示したが、それに限らず、個人ユーザ同士間または業者同士間でＥメールを送受信するものであってもよい。以下に、個人情報の不正流出者（不正漏洩者）と不正入手者との割出しを行なう監視システム、および、迷惑メール（スパム）の監視システムの発明を、まとめて説明する。

【０３５２】

従来から、個人情報の漏洩を防止する技術は多数存在しているが、一旦個人情報が漏洩した場合に、どこの業者等から漏洩したのかという漏洩主体を割出すために有効な技術は存在しなかった。さらに、その漏洩した個人情報を不正に入手した者を突き止めるために有効な技術は存在しなかった。また、迷惑メール（スパム）が送信されてきた場合に、その迷惑メール（スパム）の送信元や送信経路等をメールサーバ等に登録して、次回から同じ送信元や送信経路等を介して送信されてくる迷惑メール（スパム）を防止する技術はあった。しかし、登録する前すなわち初回の迷惑メール（スパム）の着信を防止できず、かつ、ユーザがわざわざ迷惑メール（スパム）の送信元や送信経路等をメールサーバ等に登録しなければならず、面倒であった。

【０３５３】

この監視システムの発明の目的は、個人情報の漏洩主体を割出すことを可能にすることである。また、漏洩した個人情報を不正に入手した者を突き止めることを可能にすることである。また、初回の迷惑メール（スパム）の着信を防止でき、かつ、迷惑メール（スパ

ム）の送信元や送信経路等をメールサーバ等に登録する煩雑な作業をユーザに強いることなく迷惑メール（スパム）の着信を防止することである。

【０３５４】

このよな目的を達成するべく、この監視システムの発明は、次のような手段を採用する。なお、各手段の具体例を括弧書きで挿入して示す。

【０３５５】

（１）　個人情報の漏洩を監視する監視システムであって、

相手に自己のメールアドレスを通知するときの通知用メールアドレスを生成する手段であって、通知相手を特定する情報を割出すことが可能な通知用メールアドレス（たとえば、図６１の#ｅ９¥８２%３１＆０αｔ＊ｃ）を生成するための処理を行う通知用メールアドレス生成処理手段（たとえば、図５９のＳ１０００～Ｓ１００３）と、

送信元（たとえば、図６１のＭＴＴ）から送信された電子メール（たとえば、図６１のＥメール８５）の送信先のメールアドレスが、前記通知用メールアドレス生成処理手段により生成された前記通知用メールアドレスである場合に、当該通知用メールアドレスに対応する前記通知相手を特定する情報（たとえば、図６１のＭＴＴ//○△××△）を割出し、該割出された通知相手を特定する情報と当該電子メールの送信元の情報とが一致するか否か監視する監視手段（たとえば、図６０のＳＶ５～ＳＶ１６）とを含むことを特徴とする、監視システム。

【０３５６】

このような構成によれば、通知相手に通知した通知用メールアドレスの個人情報が漏洩されて、その個人情報を不正入手した者がその個人情報としての通知用メールアドレス宛に電子メールを送信した場合に、当該電子メールの通知用メールアドレスから割出される通知相手を特定する情報と当該電子メールの送信元の情報とを比較することにより両者が一致しないことが判明でき、割出された通知相手から個人情報が漏洩した可能性が高いことと、その漏洩した個人情報を当該電子メールの送信元が不正入手した可能性が高いことを、突き止めることができる。

【０３５７】

（２）　前記通知用メールアドレス生成処理手段は、前記通知相手を特定するための通知相手特定情報（たとえば、図６１のＭＴＴ//○△××△）を含むデータを暗号化して前記通知用メールアドレスを生成するための処理を行い（たとえば、図５９のＳ１００１により暗号化してＳ１００２により鍵指定番号を分散挿入して生成し）、

前記監視手段は、前記通知用メールアドレスを復号して（たとえば、図６０のＳＶ５、ＳＶ６により共通鍵ＫＮを割出し、ＳＶ７により鍵ＫＮを用いて復号する）前記通知相手特定情報を抽出し、該通知相手特定情報と前記電子メールの送信元の情報とが一致するか否か監視する（たとえば、図６０のＳＶ８～ＳＶ１２）ことを特徴とする、（１）に記載の監視システム。

【０３５８】

このような構成によれば、通知用メールアドレスのデータ自体から通知相手特定情報を割出すことができ、たとえば通知用メールアドレス毎に対応する通知相手特定情報を登録しておく方法に比べて、多数の相手にそれぞれ通知用メールアドレスを通知した場合の通知相手特定情報の登録データ量が膨大になる不都合を防止できる。

【０３５９】

（３）　前記通知用メールアドレス生成処理手段は、前記通知相手に通知した本人のメールアドレス（たとえば、図６１の○□×△×）を含むデータを暗号化して前記通知用メールアドレスを生成する処理を行い、

前記監視手段は、前記通知用メールアドレスを復号して前記通知相手に通知した本人のメールアドレスを抽出し、監視結果適正な電子メールの場合に前記抽出した本人のメールアドレスに対応するメールボックスに当該電子メールを格納する（たとえば、図６０のＳＶ１３）ことを特徴とする、（２）に記載の監視システム。

【０３６０】

このような構成によれば、監視のために通知用メールアドレスを復号することにより、本人のメールアドレスも抽出でき、利便性が向上する。

【０３６１】

（４）　迷惑メールを監視して防止するための監視システムであって、

相手に自己のメールアドレスを通知するときの通知用メールアドレスを生成する手段であって、通知相手を特定する情報を割出すことが可能な通知用メールアドレス（たとえば、図６１の＃ｅ９￥８２％３１＆０αｔ＊ｃ）を生成するための処理を行う通知用メールアドレス生成処理手段（たとえば、図５９のＳ１０００～Ｓ１００３）と、

送信元（たとえば、図６１のＭＴＴ）から送信された電子メール（たとえば、図６１のＥメール８５）の送信先のメールアドレスが、前記通知用メールアドレス生成処理手段により生成された前記通知用メールアドレスである場合に、当該通知用メールアドレスに対応する前記通知相手を特定する情報（たとえば、図６１のＭＴＴ//○△××△）を割出し、該割出された通知相手を特定する情報と当該電子メールの送信元の情報とが一致するか否か監視する監視手段（たとえば、図６０のＳＶ５～ＳＶ１６）とを含むことを特徴とする、監視システム。

【０３６２】

このような構成によれば、通知用メールアドレスを通知した通知相手以外の者がその通知用メールアドレス宛に電子メールを送信した場合に、当該電子メールの通知用メールアドレスから割出される通知相手を特定する情報と当該電子メールの送信元の情報とを比較することにより両者が一致しないことが判明でき、その不適正な電子メールの送信を阻止することができる。

【０３６３】

（５）　前記通知用メールアドレス生成処理手段は、前記通知相手を特定するための通知相手特定情報（たとえば、図６１のＭＴＴ//○△××△）を含むデータを暗号化して前記通知用メールアドレスを生成するための処理を行い（たとえば、図５９のＳ１００１により暗号化してＳ１００２により鍵指定番号を分散挿入して生成し）、

前記監視手段は、前記通知用メールアドレスを復号して（たとえば、図６０のＳＶ５、ＳＶ６により共通鍵ＫＮを割出し、ＳＶ７により鍵ＫＮを用いて復号する）前記通知相手特定情報を抽出し、該通知相手特定情報と前記電子メールの送信元の情報とが一致するか否か監視する（たとえば、図６０のＳＶ８～ＳＶ１２）ことを特徴とする、（４）に記載の監視システム。

【０３６４】

このような構成によれば、通知用メールアドレスのデータ自体から通知相手特定情報を割出すことができ、たとえば通知用メールアドレス毎に対応する通知相手特定情報を登録しておく方法に比べて、多数の相手にそれぞれ通知用メールアドレスを通知した場合の通知相手特定情報の登録データ量が膨大になる不都合を防止できる。

【０３６５】

（６）　前記通知用メールアドレス生成処理手段は、前記通知相手に通知した本人のメールアドレス（たとえば、図６１の○□×△×）を含むデータを暗号化して前記通知用メールアドレスを生成する処理を行い、

前記監視手段は、前記通知用メールアドレスを復号して前記通知相手に通知した本人のメールアドレスを抽出し、監視結果適正な電子メールの場合に前記抽出した本人のメールアドレスに対応するメールボックスに当該電子メールを格納する（たとえば、図６０のＳＶ１３）ことを特徴とする、（５）に記載の監視システム。

【０３６６】

このような構成によれば、監視のために通知用メールアドレスを復号することにより、本人のメールアドレスも抽出でき、利便性が向上する。

【０３６７】

（７）　前記監視手段による監視の結果、前記割出された通知相手特定情報と当該電子メールの送信元の情報とが一致しない場合に（たとえば、図６０のＳＶ１２によりＮＯの

判断がなされた場合に）、当該電子メールの送信を阻止する阻止手段（たとえば、図６０のＳＶ１４～ＳＶ１６）をさらに含むことを特徴とする、（４）～（６）のいずれかに記載の監視システム。

【０３６８】

このような構成によれば、阻止手段によって迷惑メールの着信を確実に防止できる。

【０３６９】

次に、以上説明した実施の形態における変形例や特徴点等を以下に列挙する。

【０３７０】

（１）　本発明でいう「人物」の用語は、自然人に限らず法人をも含む広い概念である。本発明でいう「匿名」とは、仮想人物（ＶＰ）の氏名のことであり、仮想人物の氏名と実在人物の匿名とは同じ概念である。したがって、仮想人物の住所やＥメールアドレスや電子証明書は、実在人物が匿名でネットワーク上で行動する場合の住所，Ｅメールアドレス，電子証明書ということになる。

【０３７１】

本発明でいう「個人情報保護装置」は、装置単体ばかりでなく、複数の装置がある目的を達成するために協働するように構築されたシステムをも含む広い概念である。

【０３７２】

（２）　図１に示すように、本実施の形態では、金融機関７に、ＶＰ管理機能と、決済機能と、認証機能とを設けたが、金融機関７から、ＶＰ管理機能を分離独立させ、金融機関以外の他の守秘義務を有する所定機関にＶＰ管理機能を肩代わりさせてもよい。その肩代わりする所定機関としては、官公庁等の公共的機関であってもよい。さらに、ＲＰやＶＰに電子証明書を発行する電子証明書発行機能を、金融機関７から分離独立させ、専門の認証局に肩代わりさせてもよい。

【０３７３】

また、本実施の形態では、コンビニエンスストア２の住所をＶＰの住所としているが、その代わりに、たとえば郵便局や物流業者における荷物の集配場等をＶＰの住所としてもよい。またＶＰの住所となる専用の施設を新たに設置してもよい。

【０３７４】

ＶＰを誕生させる処理は、本実施の形態では、所定機関の一例としての金融機関７が行なっているが、本発明はこれに限らず、たとえば、ユーザ自身が自己の端末（ブラウザフォン３０等）によりＶＰを誕生（出生）させ、その誕生させたＶＰの氏名，住所，公開鍵，口座番号，Ｅメールアドレス等のＶＰ用情報を、金融機関７等の所定機関に登録するようにしてもよい。

【０３７５】

また、誕生したＶＰは、必ずしも所定機関に登録させなくてもよい。

【０３７６】

（３）　処理装置の一例としてのＩＣ端末１９Ｒまたは１９Ｖは、ＩＣカードや携帯電話あるいはＰＨＳやＰＤＡ（Personal Digital Assistant）等の携帯型端末で構成してもよい。これら携帯型端末で構成する場合には、ＶＰ用の携帯型端末とＲＰ用の携帯型端末との２種類のものを用意してもよいが、ＶＰ用モードあるいはＲＰ用モードに切換え可能に構成し、１種類の携帯型端末で事足りるように構成してもよい。

【０３７７】

図７に示したＩＣ端末１９Ｉによるアプリケーションソフトのインストールに代えて、当該アプリケーションソフトのサプライヤからネットワーク経由で当該アプリケーションソフトをブラウザフォン３０等へダウンロードするように構成してもよい。

【０３７８】

（４）　本実施の形態では、図１７に示したように、ＶＰの誕生時にそのＶＰの電子証明書が自動的に作なされて発行されるように構成したが、その代わりに、ユーザからの電子証明書の発行依頼があって初めてＶＰの電子証明書の作成発行を行なうようにしてもよい。

【０３７９】
図２３等に示すように、本実施の形態では、ＲＰの本人認証を行なう場合には、ＲＰの認証鍵ＫＮを用いるようにしたが、ＲＰが電子証明書の発行を受けている場合には、その電子証明書内の公開鍵を用いてＲＰの本人認証を行なうようにしてもよい。
【０３８０】
（５）　ブラウザフォン３０に代えて、パーソナルコンピュータを用いてもよい。
【０３８１】
トラップ型ＶＰ用に金融機関７が開設したＥメールアドレス△△△△△は、１種類のみのＥメールアドレスではなく、複数種類用意し、トラップ型ＶＰ氏名毎に使い分けるようにしてもよい。Ｓ６２０～Ｓ６２２またはＳ９６０～Ｓ９５６により、新たな匿名（トラップ型ＶＰ氏名）の生成要求があった場合に、今までに使われていない匿名を生成する新匿名生成手段が構成されている。Ｓ４３１～Ｓ４４１またはＳ９５４により、前記新匿名生成手段により生成された匿名の登録を行なう匿名登録機関（金融機関７またはＥＥＰＲＯＭ２６）に対し新たに生成された匿名の登録依頼があった場合に、該匿名を登録する匿名登録手段が構成されている。
【０３８２】
前述したＳ４５０～Ｓ４６０により、ユーザの個人情報を登録している登録機関に対しユーザから自己の個人情報の確認要求があった場合に、当該ユーザの本人認証を行なう本人認証手段（Ｓ４５２～Ｓ４５８）による本人認証の結果本人であることが確認されたことを条件として、当該ユーザに対応する個人情報を当該ユーザに送信する個人情報送信手段が構成されている。
【０３８３】
図４０（ａ）で示したトラップ型ＶＰ氏名は、サイト名（業社名）をＶＰの秘密鍵ＫＳＢで復号化したものであってもよい。
【０３８４】
つまり、Ｓ９５７により、D_{KSB}（業社名）の演算を行なってトラップ型ＶＰ氏名を生成してもよい。その場合には、Ｓ９６９により、E_{KPB}（Ｅメールの宛名）＝送信者名の演算式による判別を行なうこととなる。Ｓ９６７では、E_{KPB}（Ｅメールの宛名）が不正流出し、送信者名の業者が不正入手した旨を出力するという処理になる。
【０３８５】
（６）　前述した正当機関証明処理，正当機関チェック処理，本人証明処理，Ｓ４～Ｓ７等の本人チェック処理により、本人であることの確認を行なってなりすましを防止するための本人認証手段が構成されている。
【０３８６】
Ｓ１３～Ｓ１６により、バーチャルパーソン（仮想人物）用の電子証明書を作成して発行する仮想人物用電子証明書発行手段が構成されている。Ｓ２５～Ｓ２８により、現実世界に実在するリアルパーソン（実在人物）用の電子証明書を作成して発行する実在人物用電子証明書発行手段が構成されている。
【０３８７】
Ｓ３９～Ｓ４５により、仮想人物（バーチャルパーソン）用の銀行口座を作成するための処理を行なう銀行口座作成処理手段が構成されている。
【０３８８】
Ｓ４０～Ｓ４９により、実在人物（リアルパーソン）または仮想人物（バーチャルパーソン）用のデビットカードを発行するための処理を行なうデビットカード発行処理手段が構成されている。Ｓ５５～Ｓ６９により、仮想人物（バーチャルパーソン）に携帯される処理装置（ＶＰ用ＩＣ端末１９Ｖ）に対し、該仮想人物（バーチャルパーソン）の銀行口座内の資金の一部を引落してリロードするための処理を行なう資金引落し処理手段が構成されている。
【０３８９】
Ｓ５７～Ｓ７４により、仮想人物（バーチャルパーソン）のデビットカードを使用して

決済を行なうための処理を行なうデビットカード用決済処理手段が構成されている。Ｓ５７～Ｓ７８により、仮想人物（バーチャルパーソン）のクレジットカードを使用しての決済を行なうための処理を行なうクレジットカード用決済処理手段が構成されている。このクレジットカード用決済処理手段は、Secure Electronic Transaction（ＳＥＴ）に準拠して決済を行なう。

【０３９０】

（７）　Ｓ１４０～Ｓ１５８により、ユーザが自己の仮想人物（バーチャルパーソン）の出生依頼を行なう処理を行なうための出生依頼処理手段が構成されている。Ｓ９～Ｓ１２により、出生させる仮想人物（バーチャルパーソン）の住所であって出生依頼者である実在人物（リアルパーソン）の住所とは異なった住所を決定するための処理を行なう住所決定処理手段が構成されている。この住所決定処理手段は、コンビニエンスストアの住所を仮想人物（バーチャルパーソン）の住所として決定する。また、この住所決定処理手段は、出生依頼者である実在人物（リアルパーソン）の希望するコンビニエンスストアの住所を仮想人物（バーチャルパーソン）の住所として決定可能である。また、この住所決定処理手段は、出生依頼者である実在人物（リアルパーソン）の住所に近いコンビニエンスストアの住所を仮想人物（バーチャルパーソン）の住所として決定することが可能である。

【０３９１】

Ｓ３０５～Ｓ３１２により、ユーザに携帯される前記処理装置（ＲＰ用ＩＣ端末１９Ｒ，ＶＰ用ＩＣ端末１９Ｖ）に設けられ、当該処理装置の所有者であるユーザの実在人物（リアルパーソン）としての個人情報または仮想人物（バーチャルパーソン）としての個人情報の送信要求を受けた場合に、記憶している個人情報の中から該当する個人情報を選び出して出力する処理が可能な個人情報自動出力手段が構成されている。この個人情報自動出力手段は、送信要求の対象となっている個人情報が送信してよいものであるか否かを自動的に判別するための処理を行なう自動判別処理手段（Ｓ３０７，Ｓ３０８，Ｓ３１０，Ｓ３１１）を含んでいる。この自動判別処理手段は、どの種類の個人情報を出力してよいかをユーザが事前に入力設定でき、その入力設定に従って自動判別を行なう。またこの自動判別処理手段は、自動判別できない場合には、要求対象となっている個人情報と送信されてきたプライバシーポリシーとを出力してユーザに対し送信の許否を求めるための処理を行なう（Ｓ３０９）。

【０３９２】

コンビニエンスストア２により、仮想人物（バーチャルパーソン）がネットワーク上で購入した商品が配達されてきた場合に当該商品を預る商品預り場が構成されている。データベース１７により、前記商品預り場で商品を預る対象となる仮想人物（バーチャルパーソン）を登録しておくバーチャルパーソン登録手段が構成されている。このバーチャルパーソン登録手段は、仮想人物（バーチャルパーソン）ごとに分類して、商品を預っているか否かを特定するための預り特定情報が記憶される。さらに、当該商品の決済が済んでいるか否かを特定するための決済特定情報が記憶される。また、前記仮想人物（バーチャルパーソン）ごとに分類して当該仮想人物（バーチャルパーソン）のＥメールアドレスを記憶している。

【０３９３】

Ｓ３２３により、前記商品預り場に設けられ、商品を預っている仮想人物（バーチャルパーソン）のＥメールアドレスに対し商品を預った旨のＥメールを送信するための処理を行なうＥメール送信処理手段が構成されている。Ｓ３１７～Ｓ３４０により、前記商品預り場に設けられ、ユーザが仮想人物（バーチャルパーソン）として商品を引取りにきた場合に、当該ユーザに対し該当する商品を引渡すための処理を行なう商品引渡し処理手段が構成されている。この商品引渡し処理手段は、引取りにきたユーザの仮想人物（バーチャルパーソン）が本人であることを確認できたことを条件として引渡し処理を行なう。前記商品引き渡し処理手段は、引き渡す商品が決済済みであるか否かを判別し、決済済みでない場合には決済が行なわれたことを条件として商品の引渡し処理を行なう。

【０３９４】
（８）　前記ライフ支援センター８のサービス提供サーバ１３により、ユーザの個人情報を収集して、該個人情報に基づいて当該ユーザのライフを支援するライフ支援手段が構成されている。このライフ支援手段は、ユーザの人生の根幹をなす上位の事項（たとえばユーザの夢や人生設計）を推薦し、次にそれよりも下位の事項（たとえば職種や進路等）を推薦し、次にさらに下位の事項（たとえば趣味等）を推薦する等のように、上位から下位への順に推薦処理を行なう。さらに、ライフ支援処理手段は、推薦した事項に関連する消費支援業者（ニューミドルマン等の加盟店）を推薦する処理を行なう。その推薦の際に、収集した当該ユーザの個人情報を前記推薦した消費支援業者に提供する。
【０３９５】
（９）　可変型偽識別子生成手段（図２６のＳＤ１０、図２７のＳＥ１～ＳＥ１０、図２９のＳＧ６～ＳＧ９、図５６のＲＦＩＤ交換処理、図５７のＲＦＩＤ交換処理等）は、既に販売済みとなっている商品それぞれに付された無線識別子発信装置（ＲＦＩＤタグ）の各々が発信する識別子の範囲内で偽識別子（偽ＲＦＩＤ等）を生成する。また、図１２に示した、共通偽識別子（共通偽ＲＦＩＤ等）を生成する機能および所定個数（たとえば１個）の偽識別子（偽ＲＦＩＤ等）と当該所定個数よりも多い個数の偽識別子（偽ＲＦＩＤ等）を生成する機能を、ブラウザフォン３０にも備えてもよい。
【０３９６】
（１０）　セキュリティ用の識別子発信装置を、指輪等の形状をした携帯装置（ＩＤリング）１として個人ユーザに提供（販売）する代わりに、ＲＦＩＤタグ１ａの状態で個人ユーザに提供（販売）してもよい。その場合には、個人ユーザ自身が自己の携帯品等にＲＦＩＤタグ1aを貼着する。
【０３９７】
（１１）　図１０のコンデンサ１１０により、外部からの電源用電波を受信して動作可能となるセキュリティ用の識別子発信装置に備えられ、受信した電源用電波によって発生した電力を貯える蓄電気手段が構成されている。図１１のＳＡ６～ＳＡ１０ａにより、外部からの電源用電波が途絶えた後においても、前記蓄電気手段から供給される電力を利用して数値データを更新する数値データ更新手段が構成されている。換言すれば、図１１のＳＡ６～ＳＡ１０ａにより、外部からの電源用電波が途絶えた後においても、前記蓄電気手段から供給される電力を利用して乱数を生成する乱数生成手段が構成されている。図１１のＳＡ４により、前記数値データ更新手段から抽出された数値データを用いて偽識別子を生成する偽識別子生成手段が構成されている。換言すれば、図１１のＳＡ４により、前記乱数生成手段により生成された乱数を用いて偽識別子を生成する偽識別子生成手段が構成されている。蓄電気手段に蓄電される電力量が毎回不規則のために蓄電気手段の放電期間も不規則となり、その不規則な期間を利用して生成されたランダムな数値データ（乱数）を用いて偽識別子が生成されるため、ランダムな偽識別子を生成することができる。
【０３９８】
識別子を記憶する識別子記憶手段（図２７、図５６、図５７のＳＥ９、ＳＥ１０とＥＥＰＲＯＭ１９４等）は、交換された偽識別子を複数記憶可能である。また、交換された偽識別子をその交換順に複数記憶可能であり、上限個数の偽識別子を記憶している状態で識別子の交換が行われることにより、記憶中の最も古い偽識別子を消去する（ＳＥ９）。図２９のＳＧ９により、前記識別子記憶手段に記憶されている複数の偽識別子から発信する偽識別子を選択する手段であって、前回選択した偽識別子とは異なる偽識別子を選択可能な偽識別子選択手段が構成されている。図２９のＳＧ２により、識別子の送信要求があった場合にその旨を報知する識別子送信要求報知手段が構成されている。
【０３９９】
（１２）　図４１～図４７に基づいて説明したように、購入商品に付されている固有の識別子発信装置（ＲＦＩＤタグ）から発信される固有の識別子（ＲＦＩＤ）を利用して、当該商品に関連する種々の情報が個人ユーザに提供される。この情報提供システムは、商品メーカー３００のサーバとデータベース、商品情報サービス業者３０２のサーバとデー

タベース、中間流通業者３０１のサーバとデータベース、小売店２０ｂとからなる商品販売店のサーバとデータベースと、それらサーバ間で通信を行う通信網（広域・大容量中継網４３）から構成される。

【０４００】

商品情報サービス業者３０２のデータベースには、図４２に示すような、固有の識別子（ＲＦＩＤ）のそれぞれに対応させて、生産者、中間流通業者、小売店の各ＵＲＬが記憶されている。さらに、購入した商品に付されている固有の識別子発信装置（ＲＦＩＤタグ）から発信される固有の識別子（ＲＦＩＤ）に対応させて当該商品を購入した購入者の情報が記憶可能に構成されている。購入者が固有の識別情報（ＲＦＩＤ）を商品情報サービス業者３０２のサーバへ送信してそのサーバにアクセスすることにより、送信した固有の識別情報に対応して当該購入者の情報記録領域（購入者ページ）が設けられる。その情報記録領域（購入者ページ）に、購入者の匿名（ＶＰ名）やＶＰ住所やＥメールアドレス等を記録することができるように構成されている。またその購入者ページに、購入者が、購入商品に関するメモ書き等を書込むことができるように構成されており、購入者は商品に関する種々の情報を書込んで、固有の識別情報（ＲＦＩＤ）を商品情報サービス業者３０２のサーバへ送信してそれに対応する書込み情報を検索して閲覧できるように構成されている。

【０４０１】

図４６のＳＱ２６により、購入したい商品を当該商品に対応する固有の識別情報により特定して小売店に送信して購入予約を行う購入予約手段が構成されている。図４６のＳＱ３３、ＳＱ３５により、個人ユーザ同士で物々交換を行う物々交換手段が構成されている。図４６のＳＱ３４により、個人ユーザが自己所有の中古商品を販売するための中古商品販売手段が構成されている。図４７のＳＳ３～ＳＳ１２により、個人ユーザからの予約購入を受付けて処理するための予約購入受付処理手段が構成されている。なお、本発明でいう「識別子」とは、ＲＦＩＤに限るものではなく、それを基にプライバシーが侵害される虞の有る識別子であれば全て含む広い概念である。

【０４０２】

また、前述の実施の形態には、次のような各種構成からなる発明が記載されている。

【０４０３】

（１）　固有の識別子（ＲＦＩＤ等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

購入されることにより個人ユーザの所持品となった物品（たとえば、腕時計、眼鏡、衣服等）に付されている無線識別子発信装置（ＲＦＩＤタグ等）の固有の識別子（ＲＦＩＤ等）を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガードステップ（図１５のＳＢ１、ＳＢ３～ＳＢ７等）と、

前記個人ユーザに所持されるプライバシー保護用識別子発信装置（セキュリティ用のＲＦＩＤタグ１ａまたはブラウザフォン３０等）により、偽識別子（偽ＲＦＩＤ等）を生成する偽識別子生成ステップ（図１１のＳＡ１～ＳＡ４、または、図２６のＳＤ２、ＳＤ１０、ＳＤ１２と図２７のＳＥ１～ＳＥ１０と図２９のＳＧ３、ＳＧ３ａ、ＳＧ３ｂ、ＳＧ５～ＳＧ９、図５６、図５７等）と、

識別子の送信要求があった場合に（図１１のＳＡ１または図２９のＳＧ３によりＹＥＳの判断があった場合に）、前記偽識別子生成ステップにより生成された前記偽識別子を前記プライバシー保護用識別子発信装置から発信する発信ステップ（図１１のＳＡ５、ＳＡ１０、またはＳＧ７、ＳＧ９等）と、

識別子ガード状態となっている前記無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにする読取りステップ（図１５のＳＢ２、ＳＢ８、ＳＢ９～ＳＢ１３）とを含み、

前記偽識別子生成ステップは、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成ステップ（図２６のＳＤ１０、図２７のＳＥ１～ＳＥ１０、図２９のＳＧ６～ＳＧ９、図５６のＲＦＩＤ交換処理、図５７のＲＦＩＤ交換処理等）を含むこと

を特徴とする、プライバシー保護方法。

【０４０４】

このような構成によれば、購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にすることができ、購入済みの物品に付されている無線識別子発信装置の固有の識別子を他人により読取られてそれに基づくプライバシーの侵害が発生する不都合を極力防止することができる。しかも識別子ガード状態となっている無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにするために、購入済みの物品に付されている無線識別子発信装置の固有の識別子を利用したサービス等を個人ユーザが受けたいと思う必要な時に読取ってサービス等を享受することが可能となる。

【０４０５】

また、識別子の送信要求があった場合に、個人ユーザに所持されるプライバシー保護用識別子発信装置により偽識別子を生成して発信でき、しかも前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子の生成ができるために、複数箇所に設置された無線識別子リーダ等のそれぞれにより同一人物から発せられる偽識別子が読取られたとしても、それぞれの無線識別子リーダ等には異なった偽識別子が読取られる状態にすることができ、同一人物であることをカムフラージュできてプライバシーの侵害を極力防止することができる。

【０４０６】

（２）　固有の識別子（ＲＦＩＤ等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

プライバシー保護用識別子発信装置（セキュリティ用のＲＦＩＤタグ１ａまたはブラウザフォン３０等）を複数の個人ユーザに提供する提供ステップ（図１３等）を含み、

前記プライバシー保護用識別子発信装置は、

偽識別子（偽ＲＦＩＤ等）を生成する偽識別子生成手段（図１１のＳＡ１～ＳＡ４、または、図２６のＳＤ２、ＳＤ１０、ＳＤ１２と図２７のＳＥ１～ＳＥ１０と図２９のＳＧ３、ＳＧ３ａ、ＳＧ３ｂ、ＳＧ５～ＳＧ９、図５６、図５７等）と、

識別子の送信要求があった場合に（図１１のＳＡ１または図２９のＳＧ３によりＹＥＳの判断があった場合に）、前記偽識別子生成手段により生成された前記偽識別子を発信する発信手段（図１１のＳＡ５、ＳＡ１０、または図２９のＳＧ７、ＳＧ９等）とを含み、

前記偽識別子生成手段は、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段（図２６のＳＤ１０、図２７のＳＥ１～ＳＥ１０、図２９のＳＧ６～ＳＧ９、図５６のＲＦＩＤ交換処理、図５７のＲＦＩＤ交換処理等）を含み、

前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成して発信する前記プライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持する前記プライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子（図１３の共通偽ＲＦＩＤ等）を生成可能であり（図１２と図１３と図１１のＳＡ３、ＳＡ４、または図２６のＳＤ１０、図２７のＳＥ１～ＳＥ１０、図５６のＲＦＩＤ交換処理、図５７のＲＦＩＤ交換処理等）、

前記複数のプライバシー保護用識別子発信装置は、前記共通の偽識別子を他の偽識別子に比べて高い頻度で発信するプライバシー保護用識別子発信装置同士からなるグループであってグループ毎に前記共通の偽識別子が異なる複数のグループに分類され（図１３の千代区、新宿区、渋谷区等の各地域を指定して販売される地域毎のグループに分類され）、

前記提供ステップは、前記それぞれのグループ毎に地域を指定して該グループに属する前記プライバシー保護用識別子発信装置を個人ユーザに提供する（図１３の各地域を指定して個人ユーザに提供する）ことを特徴とする、プライバシー保護方法。

【０４０７】

このような構成によれば、プライバシー保護用識別子発信装置が複数の個人ユーザに提

供され、そのプライバシー保護用識別子発信装置は、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子の生成が可能であり、しかも、それぞれ異なった人物に所持されたプライバシー保護用識別子発信装置から発信される可変型の偽識別子には、互いに一致する共通の偽識別子が含まれるように構成されている。その結果、異なった人物から発信された識別子でありながら前記共通の識別子即ち互いに一致する識別子が発信される現象（異人物同一識別子発信現象）を生じさせることができる。このような異人物同一識別子発信現象を生じさせることのできるプライバシー保護用識別子発信装置が個人ユーザの間に普及すれば、或る地点で読取った識別子と他の地点で読取った識別子とが一致することにより同一人物であると判定して当該同一人物の個人情報を不当に収集して悪用しようとする悪意のプライバシー侵害者にとってみれば、同一の識別子を受信すればその同一識別子の発信元は同一人物であるという判定の信頼性が持てなくなる。よって、同一人物であるとの判定に基づいたプライバシー侵害行為を前提から覆すことができ、個人ユーザのプライバシーを有効に保護することが可能となる。

【０４０８】

しかも、大多数の個人ユーザが購入済み商品に付されている無線識別子発信装置から固有の識別子を発信する状態にしたままそれを所持して屋外等を歩いたとしても、一部のユーザの間でこの共通の偽識別子を発信できるプライバシー保護用識別子発信装置が普及することにより、同一人物の所持品に付された無線識別子発信装置から発信された同一の識別子が悪意のプライバシー侵害者側に複数箇所で読取られたとしても、それが同一人物であるとの信頼性を低下させることができるという撹乱効果を期待でき、このプライバシー保護用識別子発信装置を所持していない個人ユーザのプライバシーをも極力保護することが可能となる。

【０４０９】

さらに、複数のプライバシー保護用識別子発信装置は、前記共通の偽識別子を他の偽識別子に比べて高い頻度で発信するプライバシー保護用識別子発信装置同士からなるグループであってグループ毎に共通の偽識別子が異なる複数のグループに分類されており、それぞれのグループ毎に地域を指定してそのグループに属するプライバシー保護用識別子発信装置が個人ユーザに提供される。その結果、各地域内の者同士で共通の偽識別子を生成して発信する傾向が生じ、前述の異人物同一識別子発信現象を極力各地域内の個人ユーザ同士で生じさせることができ、悪意のプライバシー侵害者に対する前述した撹乱効果をより効果的に発揮することができる。

【０４１０】

（３）　固有の識別子（ＲＦＩＤ等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

プライバシー保護用識別子発信装置（セキュリティ用のＲＦＩＤタグ１ａ、またはブラウザフォン３０等）を複数の個人ユーザに提供する提供ステップ（図１３等）を含み、

前記プライバシー保護用識別子発信装置は、

偽識別子を生成する偽識別子生成手段（図１１のＳＡ１～ＳＡ４、または、図２６のＳＤ２、ＳＤ１０、ＳＤ１２と図２７のＳＥ１～ＳＥ１０と図２９のＳＧ３、ＳＧ３ａ、ＳＧ３ｂ、ＳＧ５～ＳＧ９、図５６、図５７等）と、

識別子の送信要求があった場合に（図１１のＳＡ１または図２９のＳＧ１によりＹＥＳの判断があった場合に）、前記偽識別子生成手段により生成された前記偽識別子を発信する発信手段（図１１のＳＡ５、ＳＡ１０、または図２９のＳＧ７、ＳＧ９等）とを含み、

前記偽識別子生成手段は、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段（図１１のＳＡ３、ＳＡ４、または図２６のＳＤ１０、図２７のＳＥ１～ＳＥ１０、図２９のＳＧ６～ＳＧ９、図５６のＲＦＩＤ交換処理、図５７のＲＦＩＤ交換処理等）を含み、

前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成するプライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持するプライ

バシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子（図１２のＲが０～３９に属する列のＲＦＩＤのコードデータ、図１３の共通偽ＲＦＩＤ、または図２７、図５６、図５７により互いに交換された偽ＲＦＩＤ等）を生成可能であり、

前記提供ステップにより或る個人ユーザに提供されたプライバシー保護用識別子発信装置（図１２（ａ）のテーブルを記憶しているＲＦＩＤタグ１ａ等）から、予め定められた所定個数（たとえば１個）の偽識別子を１度に発信し（図１１のＳＡ４、ＳＡ５と図１２（ａ）のＲＦＩＤ等）、

前記提供ステップにより前記或る個人ユーザとは異なる他の個人ユーザに提供されたプライバシー保護用識別子発信装置（図１２（ｂ）（ｃ）のテーブルを記憶しているＲＦＩＤタグ１ａ等）から、前記所定個数（たとえば１個）よりも多い複数（たとえば４個）の偽識別子（図１２（ｂ）（ｃ）のＲＦＩＤ１～４）を１度に発信し、該複数の偽識別子のうちの前記所定個数を除く他の偽識別子（図１２（ａ）（ｃ）のＲＦＩＤ２～４）を前記共通の偽識別子として生成することを特徴とする、プライバシー保護方法。

【０４１１】

このような構成によれば、プライバシー保護用識別子発信装置が複数の個人ユーザに提供され、そのプライバシー保護用識別子発信装置は、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子の生成が可能であり、しかも、それぞれ異なった人物に所持されたプライバシー保護用識別子発信装置から発信される可変型の偽識別子には、互いに一致する共通の偽識別子が含まれるように構成されている。その結果、異なった人物から発信された識別子でありながら前記共通の識別子即ち互いに一致する識別子が発信される現象（異人物同一識別子発信現象）を生じさせることができる。このような異人物同一識別子発信現象を生じさせることのできるプライバシー保護用識別子発信装置が個人ユーザの間に普及すれば、或る地点で読取った識別子と他の地点で読取った識別子とが一致することにより同一人物であると判定して当該同一人物の個人情報を不当に収集して悪用しようとする悪意のプライバシー侵害者にとってみれば、同一の識別子を受信すればその同一識別子の発信元は同一人物であるという判定の信頼性が持てなくなる。よって、同一人物であるとの判定に基づいたプライバシー侵害行為を前提から覆すことができ、個人ユーザのプライバシーを有効に保護することが可能となる。

【０４１２】

しかも、大多数の個人ユーザが購入済み商品に付されている無線識別子発信装置から固有の識別子を発信する状態にしたままそれを所持して屋外等を歩いたとしても、一部のユーザの間でこの共通の偽識別子を発信できるプライバシー保護用識別子発信装置が普及することにより、同一人物の所持品に付された無線識別子発信装置から発信された同一の識別子が悪意のプライバシー侵害者側に複数箇所で読取られたとしても、それが同一人物であるとの信頼性を低下させることができるという撹乱効果を期待でき、このプライバシー保護用識別子発信装置を所持していない個人ユーザのプライバシーをも極力保護することが可能となる。

【０４１３】

また、或る個人ユーザに提供されたプライバシー保護用識別子発信装置から予め定められた所定個数の偽識別子が一度に発信される一方、前記或る個人ユーザとは異なる他の個人ユーザに提供されたプライバシー保護用識別子発信装置から前述の所定個数よりも多い複数の偽識別子が一度に発信され、その複数の偽識別子の内の前記所定個数を除く他の偽識別子が前述の共通の偽識別子として生成されて発信される。その結果、個人ユーザに携帯された購入済物品に付されている無線識別子発信装置が常時識別子が発信される状態になっていたとしても、前述の異人物同一識別子発信現象を生じさせることができる。

【０４１４】

つまり、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザが偽識別子を発信するプライバシー保護用識別子発信装置を所持した場合には、購入済の所持品に付されている無線識別子発信装置とプライバシー保護用識別子発信装置との両方から識別子が発信されることとなり、１度に

複数の識別子が発信される状態となる。そして、その複数の識別子中の一部が可変型であり他の一部が変化しない固定型となる。つまり、複数箇所で識別子が読取られた時にはそれぞれに読取られた複数の識別子中の所定個数のもののみが可変型の異なった偽識別子となりその他のものは携帯品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象（複数識別子中所定個数可変型現象）が生ずる。その結果、この複数識別子中所定個数可変型現象が生じれば同一人物であることが見破られてしまう不都合が生じる。

【０４１５】

そこで本発明では、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザに前述の所定個数の偽識別子を一度に発信する少数識別子発信タイプのプライバシー保護用識別子発信装置を提供し、購入済の所持品から固有の識別子が他人に読取られない状態になっている個人ユーザに対し前記所定個数よりも多い複数の偽識別子を一度に発信する多数識別子発信タイプのプライバシー保護用識別子発信装置を提供する。その結果、前者の個人ユーザからは、所定個数の偽識別子と携帯している購入済所持品の無線識別子発信装置から発信される固有の識別子とが同時に発信される一方、後者の個人ユーザからは、前者の個人ユーザから発信される偽識別子よりも多い偽識別子が一度に発信され、その多い偽識別子の内前者の個人ユーザから発信される偽識別子の個数（所定個数）を除く他の偽識別子が前述の共通の偽識別子として生成されて発信されることとなる。これにより、前者の個人ユーザの場合には、複数箇所で識別子が読取られた時にはそれぞれに読取られた複数の識別子中の前記所定個数のもののみが可変型の異なった偽識別子となりその他のものは携帯品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象（複数識別子中所定個数可変型現象）が生ずる。一方、多数識別子発信タイプのプライバシー保護用識別子発信装置を所持する後者のユーザ同士の間では、複数発信された偽識別子の内前記所定個数を除く他の偽識別子が前述の共通の偽識別子として生成されて発信可能であるために、やはり複数識別子中所定個数可変型現象が生ずる。しかもこの現象は、異なった人物の間で生ずる。

【０４１６】

以上より、前述の複数識別子中所定個数可変型現象が生じたとしてもそれが必ずしも同一人物間で生ずるとは限らず、異なった人物の間でも生ずる現象となり、悪意のプライバシー侵害者による複数識別子中所定個数可変型現象に基づく同一人物であるとの推測の信頼性を低下させることができ、プライバシーを極力保護することができる。

【０４１７】

（４）　固有の識別子（ＲＦＩＤ等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護用識別子発信装置（セキュリティ用のＲＦＩＤタグ１ａまたはブラウザフォン３０等）であって、

プライバシー保護用の偽識別子を生成する手段であって、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段（図１１のＳＡ１～ＳＡ４、または、図２６のＳＤ２、ＳＤ１０、ＳＤ１２と図２７のＳＥ１～ＳＥ１０と図２９のＳＧ３、ＳＧ３ａ、ＳＧ３ｂ、ＳＧ５～ＳＧ９、図５６、図５７等）と、

識別子の送信要求があった場合に（図１１のＳＡ１または図２９のＳＧ３によりＹＥＳの判断があった場合に）、前記可変型偽識別子生成手段により生成された偽識別子を発信する発信手段（図１１のＳＡ５、ＳＡ１０、またはＳＧ７、ＳＧ９等）とを含むことを特徴とする、プライバシー保護用識別子発信装置。

【０４１８】

このような構成によれば、識別子の送信要求があった場合に、個人ユーザに所持されるプライバシー保護用識別子発信装置により偽識別子を生成して発信でき、しかも前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子の生成ができるために、複数箇所に設置された無線識別子リーダ等のそれぞれにより同一人物から発せられる偽識別子が読取られたとしても、それぞれの無線識別子リーダ等には異なった偽識別子が読取ら

れる状態にすることができ、同一人物であることをカムフラージュできてプライバシーの侵害を極力防止することができる。

【０４１９】

（５）　前記可変型偽識別子生成手段は、既に販売済みとなっている商品それぞれに付された無線識別子発信装置（ＲＦＩＤタグ等）の各々が発信する識別子の範囲内で前記偽識別子を生成することを特徴とする、（４）に記載のプライバシー保護用識別子発信装置。

【０４２０】

このような構成によれば、既に販売済みとなっている商品それぞれに付された無線識別子発信装置の各々が発信する識別子の範囲内で可変型の偽識別子が生成されて発信されるために、発信された偽識別子が既に消費者の購入済み商品に付された無線識別子発信装置から発信される識別子と区別することができず、発信された識別子が偽の識別子であると見破られてしまう不都合を極力防止することができる。

【０４２１】

（６）　前記発信手段は、前回の偽識別子の発信から所定時間内（たとえば５秒内）に再度識別子の送信要求があった場合に、前回発信した偽識別子と同じ偽識別子を発信する（図１１のＳＡ２、ＳＡ１０、または図２９のＳＧ３ａ、ＳＧ３ｂ等）ことを特徴とする、（４）または（５）に記載のプライバシー保護用識別子発信装置。

【０４２２】

このような構成によれば、発信手段が、前回の識別子の発信から所定時間内に再度識別子の送信要求があった場合に前回発信した識別子と同じ識別子を発信するために、識別子読取装置側における読取り制度の信頼性の向上等のために複数回連続して識別子の発信要求を送信して連続して複数回識別子を読取る方式が採用されたとしても、同じ偽識別子が発信されるために、連続して複数回読取られた識別子が異なることによる不都合を極力防止することができる。また、可変型の偽識別子であるかまたは本物の無線識別子発信装置から発信された固有の識別子であるかをチェックすることを目的として、前述と同様に複数回連続して識別し発信要求を送信して連続的に識別子を読取ることが行われたとしても、可変型の偽識別子であることが見破られてしまう不都合を極力防止することができる。

【０４２３】

（７）　前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成するプライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持するプライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子を生成可能（図１２のＲが０～３９の領域に属する列のＲＦＩＤを生成可能、または図２７や図５６や図５７のＲＦＩＤ交換処理で互いに交換した偽ＲＦＩＤを生成可能）であることを特徴とする、（４）～（６）のいずれかに記載のプライバシー保護用識別子発信装置。

【０４２４】

このような構成によれば、それぞれ異なった人物に所持されたプライバシー保護用識別子発信装置から発信される可変型の偽識別子には、互いに一致する共通の偽識別子が含まれるように構成されている。その結果、異なった人物から発信された識別子でありながら前記共通の識別子即ち互いに一致する識別子が発信される現象（異人物同一識別子発信現象）を生じさせることができる。このような異人物同一識別子発信現象を生じさせることのできるプライバシー保護用識別子発信装置が個人ユーザの間に普及すれば、或る地点で読取った識別子と他の地点で読取った識別子とが一致することにより同一人物であると判定して当該同一人物の個人情報を不当に収集して悪用しようとする悪意のプライバシー侵害者にとってみれば、同一の識別子を受信すればその同一識別子の発信元は同一人物であるという判定の信頼性が持てなくなる。よって、同一人物であるとの判定に基づいたプライバシー侵害行為を前提から覆すことができ、個人ユーザのプライバシーを有効に保護することが可能となる。

【０４２５】

しかも、大多数の個人ユーザが購入済み商品に付されている無線識別子発信装置から固有の識別子を発信する状態にしたままそれを所持して屋外等を歩いたとしても、一部のユーザの間でこの共通の偽識別子を発信できるプライバシー保護用識別子発信装置が普及することにより、同一人物の所持品に付された無線識別子発信装置から発信された同一の識別子が悪意のプライバシー侵害者側に複数箇所で読取られたとしても、それが同一人物であるとの信頼性を低下させることができるという撹乱効果を期待でき、このプライバシー保護用識別子発信装置を所持していない個人ユーザのプライバシーをも極力保護することが可能となる。

【０４２６】

（８）　他のプライバシー保護用識別子発信装置（ブラウザフォン３０等）と交信する交信手段（図２７、図５６、図５７のＲＦＩＤ交換処理）をさらに含み、

前記可変型偽識別子生成手段は、識別子を記憶する識別子記憶手段（図２７、図５６、図５７のＳＥ９、ＳＥ１０とＥＥＰＲＯＭ１９４等）を含み、

前記交信手段は、前記他のプライバシー保護用識別子発信装置と交信して（図２７の直接電波交信、図５６の通話交信、図５７の電子メール交信等）、前記識別子記憶手段に記憶している前記識別子を前記他のプライバシー保護用識別子発信装置に送信するとともに（図２７のＳＥ６、ＳＥ８、または図５６のＳＳ８、ＳＥ９、ＳＥ１０、または図５７のＳＥ６、ＳＴ３等）当該他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させて（図２７のＳＥ７～ＳＥ１０、または図５６のＳＥ７、ＳＳ８、または図５７のＳＴ８、ＳＥ９、ＳＥ１０等）、記憶している互いの識別子を交換し、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に（図２９のＳＧ３によりＹＥＳの判断があった場合に）、前記識別子記憶手段に記憶している交換後の識別子を読出すことにより前記共通の偽識別子として生成する（図２９のＳＧ９等）ことを特徴とする、（７）に記載のプライバシー保護用識別子発信装置。

【０４２７】

このような構成によれば、プライバシー保護用識別子発信装置同士で交信して、互いに記憶している識別子同士を送受信して互いの識別子を交換する。そして、識別子の送信要求があった場合には、前述した交換後の識別子が前述の共通の偽識別子として生成されて発信される。その結果、互いに交信して識別しを交換するという比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

【０４２８】

なお、１度に発信される複数の識別子同士を交換し、識別子の送信要求があった場合に、該複数の識別子を1度に全て発信してもよいが、該複数の識別子の内の所定個数を他の偽識別子（たとえば乱数を利用して生成されたランダムな偽識別子）に変換する変換手段を設け、変換した後の状態の複数の識別子を発信するようにし、前述の異人物間での複数識別子中所定個数可変型現象が生じるようにしてもよい。

【０４２９】

（９）　前記交信手段は、互いの識別子を交換するときの交信可能通信限界距離が２０メートル以内に定められており、該交信可能通信限界距離圏内に進入した他のプライバシー保護用識別子発信装置と交信して互いの識別子を交換する（図２７のＳＥ１、ＳＥ２等）ことを特徴とする、（８）に記載のプライバシー保護用固有識別子発信装置。

【０４３０】

このような構成によれば、互いの識別子を交換するときの交信可能通信限界距離が２０メートル以内に定められており、その交信可能通信限界距離圏内に進入したプライバシー保護用識別子発信装置と互いに交信して識別子が交換されるために、２０メートル以内という比較的近距離圏内に位置する個人ユーザの間で互いの識別子の交換がなされることとなり、比較的近くに位置していた者同士で共通の偽識別子を共有して発信できる状態となり、前述の異人物同一識別子発信現象を極力近距離圏内に位置していた個人ユーザ同士で

生じさせることができ、悪意のプライバシー侵害者に対する前述した撹乱効果をより効果的に発揮することができる。

【０４３１】

（１０）　前記交信手段は、既に交信して前記識別子の交換を行なった他のプライバシー保護用識別子発信装置と所定期間内（たとえば１日以内）に再度前記識別子の交換を行なうことを禁止する禁止手段（図２７図、図５６、図５７のＳＥ３等）を有することを特徴とする、（８）または（９）に記載のプライバシー保護用識別子発信装置。

【０４３２】

このような構成によれば、既に交信して識別子の交換を行なった他のプライバシー保護用識別子発信装置と所定期間内に再度識別子の交換を行なうことを防止でき、既に識別子交換済みの相手と所定期間内に再度識別子の交換を行なうという無駄を防止することができる。

【０４３３】

（１１）　前記交信手段は、電話機能（ブラウザフォン３０による通話機能）を有しており、電話で交信した他のプライバシー保護用識別子発信装置と互いの識別子を交換し（図５６のＲＦＩＤ交換処理等）、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している交換後の識別子を読出すことにより前記共通の偽識別子として生成する（図２９のＳＧ９）ことを特徴とする、（８）～（１０）のいずれかに記載のプライバシー保護用識別子発信装置。

【０４３４】

このような構成によれば、交信手段が電話機能を有しており、電話で交信した他のプライバシー保護用識別子発信装置と互いの識別子の交換を行なうために、比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

【０４３５】

（１２）　前記交信手段は、電子メール機能（ブラウザフォン３０によるＥメール機能等）を有しており、電子メールの送信とともに前記識別子記憶手段に記憶している識別子を他のプライバシー保護用識別子発信装置に送信し（図５７のＳＥ５、ＳＥ６、ＳＴ３等）、電子メールの受信とともに他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させ（図５７のＳＴ８、ＳＥ９、ＳＥ１０等）、

前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している他のプライバシー保護用識別子発信装置から送信されてきた識別子を読出すことにより前記共通の偽識別子として生成する（図２９のＳＧ９）ことを特徴とする、（８）～（１１）のいずれかに記載のプライバシー保護用識別子発信装置。

【０４３６】

このような構成によれば、交信手段が電子メール機能を有しており、電子メールの送信とともに識別子記憶手段に記憶している識別子を他のプライバシー保護用識別子発信装置に送信し、電子メールの受信とともに他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して識別子記憶手段に記憶させることにより互いの識別子の交換を行なうために、比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

【０４３７】

（１３）　前記発信手段は、他のプライバシー保護用識別子発信装置（図１２（ａ）のテーブルを記憶しているＲＦＩＤタグ１ａ等）から１度に発信される所定個数（たとえば１個）の偽識別子よりも多い複数の偽識別子を１度に発信可能であり（図１２（ｂ）（ｃ）の４個のＲＦＩＤ１～４、図１１のＡＳ４、ＡＳ５等）、

前記可変型偽識別子生成手段は、前記複数の偽識別子のうちの前記所定個数（たとえば１個）を除く他の偽識別子を前記共通の偽識別子として生成する（図１２（ａ）（ｃ）の

ＲＦＩＤ２～４を共通の偽ＲＦＩＤとして生成する）ことを特徴とする、（４）～（１２）のいずれかに記載のプライバシー保護用識別子発信装置。

【０４３８】

このような構成によれば、或る個人ユーザに提供されたプライバシー保護用識別子発信装置から予め定められた所定個数の偽識別子が１度に発信される一方、前記或る個人ユーザとは異なる他の個人ユーザに提供されたプライバシー保護用識別子発信装置から前記所定個数よりも多い複数の偽識別子が一度に発信され、その複数の偽識別子の内の前記所定個数を除く他の偽識別子が前記共通の偽識別子として生成されて発信される。その結果、個人ユーザに所持された購入済物品から他人が固有の識別子を読取ることのできる状態になっていたとしても、前述の異人物同一識別子発信現象を生じさせることができる。

【０４３９】

つまり、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザが偽識別子を発信するプライバシー保護用識別子発信装置を所持した場合には、購入済の所持品に付されている無線識別子発信装置とプライバシー保護用識別子発信装置との両方から識別子が発信されることとなり、１度に複数の識別子が発信される状態となる。そして、その複数の識別子中の一部が可変型であり他の一部が変化しない固定型となる。つまり、複数箇所で識別子が読取られた時にはそれぞれに読取られた複数の識別子中の所定個数のもののみが可変型の異なった偽識別子となりその他のものは携帯品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象（複数識別子中所定個数可変型現象）が生ずる。その結果、この複数識別子中所定個数可変型現象が生じれば同一人物であることが見破られてしまう不都合が生じる。

【０４４０】

そこで本発明では、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザに前記所定個数の偽識別子を一度に発信する少数識別子発信タイプのプライバシー保護用識別子発信装置を提供し、購入済の所持品から固有の識別子が他人に読取られない状態になっている個人ユーザに対し前記所定個数よりも多い複数の偽識別子を一度に発信する多数識別子発信タイプのプライバシー保護用識別子発信装置を提供する。その結果、前者の個人ユーザからは、所定個数の偽識別子と購入済所持品の無線識別子発信装置から発信される固有の識別子とが同時に発信される一方、後者の個人ユーザからは、前者の個人ユーザが発信される偽識別子よりも多い偽識別子が一度に発信され、その多い偽識別子の内前者の個人ユーザから発信される偽識別子の個数（所定個数）を除く他の偽識別子が前述の共通の偽識別子として生成されて発信されることとなる。これにより、前者の個人ユーザの場合には、複数箇所で識別子が読取られた時にはそれぞれに読取られた複数の識別子中の前記所定個数のもののみが可変型の異なった偽識別子となりその他のものは所持品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象（複数識別子中所定個数可変型現象）が生ずる。一方、多数識別子発信タイプのプライバシー保護用識別子発信装置を所持する後者のユーザ同士の間では、複数発信された偽識別子の内前記所定個数を除く他の偽識別子が前述の共通の偽識別子として生成されて発信可能であるために、やはり複数識別子中所定個数可変型現象が生ずる。しかもこの現象は、異なった人物の間で生ずる。

【０４４１】

以上より、前述の複数識別子中所定個数可変型現象が生じたとしてもそれが必ずしも同一人物で生ずるとは限らず、異なった人物の間でも生ずる現象となり、悪意のプライバシー侵害者による複数識別子中所定個数可変型現象に基づく同一人物であるとの推測の信頼性を低下させることができ、プライバシーを極力保護することができる。

【０４４２】

（１４）　購入されることにより個人ユーザの所持品となった物品（たとえば、腕時計、眼鏡、衣服等）に付されている無線識別子発信装置（ＲＦＩＤタグ等）の固有の識別子

（ＲＦＩＤ等）を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガード手段（図１５のＳＢ１、ＳＢ３～ＳＢ７等）と、

識別子ガード状態となっている前記無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにする読取り手段（図１５のＳＢ２、ＳＢ８、ＳＢ９～ＳＢ１３）とを、さらに含むことを特徴とする、（４）～（１３）のいずれかに記載のプライバシー保護用識別子発信装置。

【０４４３】

このような構成によれば、購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にすることができ、購入済みの物品に付されている無線識別子発信装置の固有の識別子を他人により読取られてそれに基づくプライバシーの侵害が発生する不都合を極力防止することができる。しかも識別子ガード状態となっている無線識別子発信装置の識別子を 個人ユーザの意思に従って読取ることができるようにするために、購入済みの物品に付されている無線識別子発信装置の固有の識別子を利用したサービス等を個人ユーザが受けたいと思う必要なときに読取ってサービス等を享受することが可能となる。

【０４４４】

（１５）　前記識別子ガード手段は、本人認証のための固有識別情報（たとえばパスワード）を発信して前記無線識別子発信装置に認証させて本人確認ができない限り識別子を発信しない識別子発信停止状態に切換え（図１５のＳＢ３～ＳＢ８等）、

前記読取り手段は、前記固有識別情報を発信して前記無線識別子発信装置に本人認証を行なわせた上で識別子を発信可能状態にする（図１５のＳＢ８、ＳＢ９～ＳＢ１３等）ことを特徴とする、（１４）に記載のプライバシー保護用識別子発信装置。

【０４４５】

このような構成によれば、識別子ガード手段により、本人認証のための固有識別情報を発信して前記無線識別子発信装置に認証させて本人確認ができない限り識別子を発信しない識別子発信停止状態に切換え、読取り手段により、固有識別情報を発信して無線識別子発信装置に本人認証を行なわせた上で識別子を発信可能状態にするために、確実に無線識別子発信装置の識別子をガードした状態にできるとともに、本人認証が行われた本人のみが無線識別子発信装置を識別子発信可能状態にすることができ、セキュリティを向上させることができる。

【０４４６】

（１６）　固有の識別子（ＲＦＩＤ等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護方法であって、

個人ユーザのプライバシーを保護するために匿名（トラップ型バーチャルパーソンＥ（Ｂ１３Ｐ）等）を名乗り匿名ユーザ（トラップ型バーチャルパーソン）として行動するために作成された匿名（Ｅ（Ｂ１３Ｐ）等）と該個人ユーザとの対応関係を特定可能な情報を守秘義務のある所定機関（金融機関７等）において登録する処理を行なう登録処理ステップ（図１７のＳ１５、図１９のＳ４４０等）と、

前記匿名ユーザ用の電子証明書を発行する電子証明書発行ステップ（図１７のＳ１７、図１９のＳ４４１等）と、

前記匿名ユーザの住所を、該匿名に対応する個人ユーザとは異なった住所に設定するための住所設定ステップ（図１７のＳ９～Ｓ１２等）と、

所定の業者（たとえば、百貨店等の商品販売業者等）にユーザ登録するときに（たとえばポイントカードの新規発行時の顧客登録のときに）前記匿名の情報を登録して前記匿名ユーザとして登録するユーザ登録ステップ（図３２（ｂ）のＳＪ１～ＳＪ８と図３３のＳＫ２、ＳＫ２１～ＳＫ２４、ＳＫ１８～ＳＫ２０等）と、

識別子の送信要求があった場合に（図２９のＳＧ３によりＹＥＳの判断があった場合に）、前記個人ユーザに所持されるプライバシー保護用識別子発信装置（ブラウザフォン３０等）から偽識別子を発信する発信ステップ（図２９のＳＧ３～ＳＧ１３等）と、

前記ユーザ登録ステップにより前記匿名を登録した前記業者に対応する匿名用偽識別子を記憶する匿名用偽識別子記憶手段（図３２のＳＪ８、図９、ＥＥＰＲＯＭ２６等）とを含み、

前記発信ステップは、前記匿名を登録している前記業者に対し前記偽識別子を発信する場合には該業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する（図２９のＳＧ４、ＳＧ１０～ＳＧ１２等）ことを特徴とする、プライバシー保護方法。

【０４４７】

このような構成によれば、個人ユーザのプライバシーを保護するために匿名を作成しその匿名を名乗って行動する匿名ユーザ用の電子証明書が発行されるため、匿名ユーザでありながらも発行された電子証明書を提示することにより売買等の取引き行為の主体になることが可能となる。しかも、匿名ユーザの住所が、該匿名に対応する個人ユーザとは異なった住所に設定されているために、住所を手がかりにどの個人ユーザがどの匿名ユーザに該当するのかを見破られてしまう不都合も極力防止できる。また、所定の業者にユーザ登録するときに匿名の情報を登録して匿名ユーザとして登録するため、該業社に対して匿名を名乗り匿名ユーザとして行動することができ、個人ユーザ本人のプライバシーを守りながらも該業社に対し売買等の取引き行為を行なうことができるとともに、ユーザ登録によるサービス等を享受することができる。

【０４４８】

一方、匿名を登録した業社に対して匿名ユーザとして行動しているときに該匿名ユーザから発信された識別子がその業社側に読取られた場合には、業社側がその識別子を匿名ユーザの匿名情報に対応付けて記憶する虞がある。そうすることにより業社側は、たとえば、移動する匿名ユーザから発せられる識別情報を要所要所で読取って移動軌跡を収集分析して顧客情報を蓄積することにより、マーケティング等に活用できるという利点がある。しかし、ユーザが匿名ユーザとして行動するときと通常の個人ユーザとして行動するときとで同じ識別子を発信したのでは、その識別子を手がかりにどの匿名ユーザがどの通常の個人ユーザか見破られてしまう虞がある。本発明では、匿名を登録した業者に対応する匿名用偽識別子が匿名用偽識別子記憶手段に記憶されており、匿名を登録している業者に対し偽識別子を発信する場合には該業者に対応する匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信するため、匿名用偽識別子と通常の個人ユーザから発信される識別子とを別々のものにすることができ、識別子を手がかりに、どの匿名ユーザがどの通常の個人ユーザか見破られてしまう不都合を極力防止できる。

【０４４９】

（１７）　前記発信ステップは、前記匿名を登録している前記業者に対し前記偽識別子を発信する場合でないときであっても（図２９のＳＧ１０によりＮＯの判断がなされるときであっても）、前記匿名用偽識別子を発信する旨の個人ユーザの操作があった場合には（図２８のＳＦ７ａによりＹＥＳの判断がなされＳＦ７ｂにより業者の選択指定が記憶された場合には）、前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する（図２９のＳＧ１３等）ことを特徴とする、（１６）に記載のプライバシー保護方法。

【０４５０】

このような構成によれば、匿名を登録している業者に対し偽識別子を発信する場合でないときであっても、匿名用偽識別子を発信する旨の個人ユーザの操作があった場合には、匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信することができる。その結果、その匿名用識別子を受信した業社から該匿名用識別子に対応する匿名宛にダイレクトメールや電子メールが送られてきた場合には、その匿名をユーザ登録している業社からメールを送ってきた業社に匿名情報が横流しされたことが判明でき、個人情報の横流しを監視することが可能となる。

【０４５１】

（１８）　固有の識別子（ＲＦＩＤ等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護システムであって、

個人ユーザのプライバシーを保護するために匿名（トラップ型バーチャルパーソンＥ（Ｂ１３Ｐ）等）を名乗り匿名ユーザ（トラップ型バーチャルパーソン）として行動するために作成された匿名（Ｅ（Ｂ１３Ｐ）等）と該個人ユーザとの対応関係を特定可能な情報を守秘義務のある所定機関（金融機関７等）において登録する処理を行なう登録処理手段（図１７のＳ１５、図１９のＳ４４０等）と、

所定の業者（たとえば、百貨店等の商品販売業者等）にユーザ登録するときに（たとえばポイントカードの新規発行時の顧客登録のときに）前記匿名の情報を登録して前記匿名ユーザとして登録するユーザ登録手段（図３２（ｂ）のＳＪ１～ＳＪ８と図３３のＳＫ２、ＳＫ２１～ＳＫ２４、ＳＫ１８～ＳＫ２０等）と、

識別子の送信要求があった場合に（図２９のＳＧ３によりＹＥＳの判断があった場合に）、前記個人ユーザに所持されるプライバシー保護用識別子発信装置（ブラウザフォン３０等）から偽識別子を発信する発信手段（図２９のＳＧ３～ＳＧ１３等）と、

前記ユーザ登録手段により前記匿名を登録した前記業者に対応する匿名用偽識別子を記憶する匿名用偽識別子記憶手段（図３２のＳＪ８、図９、ＥＥＰＲＯＭ２６等）とを含み、

前記発信手段は、前記匿名を登録している前記業者に対し前記偽識別子を発信する場合には該業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する（図２９のＳＧ４、ＳＧ１０～ＳＧ１２等）ことを特徴とする、プライバシー保護システム。

【０４５２】

このような構成によれば、所定の業者にユーザ登録するときに匿名の情報を登録して匿名ユーザとして登録するため、該業社に対して匿名を名乗り匿名ユーザとして行動することができ、個人ユーザ本人のプライバシーを守りながらもユーザ登録によるサービス等を享受することができる。

【０４５３】

一方、匿名を登録した業社に対して匿名ユーザとして行動しているときに該匿名ユーザから発信された識別子がその業社側に読取られた場合には、業社側がその識別子を匿名ユーザの匿名情報に対応付けて記憶する虞がある。そうすることにより、たとえば、業社側は移動する匿名ユーザから発せられる識別情報を要所要所で読取って移動軌跡を収集分析して顧客情報を蓄積することにより、マーケティング等に活用できるという利点がある。しかし、ユーザが匿名ユーザとして行動するときと通常の個人ユーザとして行動するときとで同じ識別子を発信したのでは、その識別子を手がかりにどの匿名ユーザがどの通常の個人ユーザか見破られてしまう虞がある。本発明では、匿名を登録した業者に対応する匿名用偽識別子が匿名用偽識別子記憶手段に記憶されており、匿名を登録している業者に対し偽識別子を発信する場合には該業者に対応する匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信するため、匿名用偽識別子と通常の個人ユーザから発信される識別子とを別々のものにすることができ、識別子を手がかりに、どの匿名ユーザがどの通常の個人ユーザか見破られてしまう不都合を極力防止できる。

【０４５４】

（１９）　固有の識別子（ＲＦＩＤ）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護用識別子発信装置（ブラウザフォン３０等）であって、

所定の業者（たとえば、百貨店等の商品販売業者等）に対し個人ユーザが匿名（トラップ型バーチャルパーソンＥ（Ｂ１３Ｐ）等）を名乗り匿名ユーザ（トラップ型バーチャルパーソン）として行動する場合に前記業者に対応する匿名用偽識別子を記憶する匿名用偽識別子記憶手段（図３２のＳＪ８、図９、ＥＥＰＲＯＭ２６等）と

識別子の送信要求があった場合に（図２９のＳＧ３によりＹＥＳの判断があった場合に）偽識別子を発信する手段であって、前記業者に対し前記偽識別子を発信する場合には該業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する発信手段（図２９のＳＧ４、ＳＧ１０～ＳＧ１２等）とを含むことを特徴とする、プライ

バシー保護用識別子発信装置。

【０４５５】

このような構成によれば、所定の業者に対し個人ユーザが匿名を名乗り匿名ユーザとして行動する場合に前記業者に対応する匿名用偽識別子が匿名用偽識別子記憶手段に記憶されており、識別子の送信要求があった場合に、前記業者に対し偽識別子を発信する場合には該業者に対応する匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信する。業社に対して匿名ユーザとして行動しているときに該匿名ユーザから発信された識別子がその業社側に読取られた場合には、業社側がその識別子を匿名ユーザの匿名情報に対応付けて記憶する虞がある。そうすることにより、たとえば、業社側は移動する匿名ユーザから発せられる識別情報を要所要所で読取って移動軌跡を収集分析して顧客情報を蓄積することにより、マーケティング等に活用できるという利点がある。しかし、ユーザが匿名ユーザとして行動するときと通常の個人ユーザとして行動するときとで同じ識別子を発信したのでは、その識別子を手がかりにどの匿名ユーザがどの通常の個人ユーザか見破られてしまう虞がある。本発明では、前記業者に対応する匿名用偽識別子が匿名用偽識別子記憶手段に記憶されており、前記業者に対し偽識別子を発信する場合には該業者に対応する匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信するため、匿名用偽識別子と通常の個人ユーザから発信される識別子とを別々のものにすることができ、識別子を手がかりに、どの匿名ユーザがどの通常の個人ユーザか見破られてしまう不都合を極力防止できる。

【０４５６】

（２０）　前記発信手段は、個人ユーザが匿名を名乗る前記業者に対し前記偽識別子を発信する場合でないときであっても（図２９のＳＧ１０によりＮＯの判断がなされるときであっても）、前記匿名用偽識別子を発信する旨の個人ユーザの操作があった場合には（図２８のＳＦ７ａによりＹＥＳの判断がなされＳＦ７ｂにより業者の選択指定が記憶された場合には）、前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する（図２９のＳＧ１３等）ことを特徴とする、（１９）に記載のプライバシー保護用識別子発信装置。

【０４５７】

このような構成によれば、個人ユーザが匿名を名乗る前記業者に対し前記偽識別子を発信する場合でないときであっても、匿名用偽識別子を発信する旨の個人ユーザの操作があった場合には、匿名用偽識別子を匿名用偽識別子記憶手段から読出して発信することができる。その結果、その匿名用識別子を受信した業社から該匿名用識別子に対応する匿名宛にダイレクトメールや電子メールが送られてきた場合には、個人ユーザが匿名を名乗る前記業者からメールを送ってきた業社に匿名情報が横流しされたことが判明でき、個人情報の横流しを監視することが可能となる。

【０４５８】

（２１）　前記所定の業者は、商品を販売する販売店（図３０の百貨店２０６等）であり、

前記匿名用偽識別子記憶手段は、前記販売店においてポイントカードの発行に伴うユーザ登録の際に匿名ユーザとして登録した当該販売店に対応する匿名用偽識別子を記憶しており（図３２のＳＪ８、図９参照）、

前記発信手段は、前記販売店において購入した商品に付されている無線識別子発信装置から発信される固有の識別子を利用して割出される当該商品の価格を支払うための自動決済を行う際に（図３１の自動決済処理を行う際に）、前記無線識別子発信装置の前記固有の識別子を読取るための識別子送信要求があった場合に（図２９のＳＧ１０によりＹＥＳの判断がなされた場合に）、前記匿名用偽識別子を前記匿名用偽識別子記憶手段から読出して発信する（図２９のＳＧ４、ＳＧ１０～ＳＧ１２等）ことを特徴とする、（１９）または（２０）に記載のプライバシー保護用識別子発信装置。

【０４５９】

このような構成によれば、販売店においてポイントカードの発行に伴うユーザ登録の際

に匿名ユーザとして登録することにより、当該販売店において匿名ユーザとして行動して商品購入等を行なうことができ、個人ユーザのプライバシーを保護しながらもポイント付与のサービスも享受できる。また、販売店において購入した商品に付されている無線識別子発信装置から発信される固有の識別子を利用して割出される当該商品の価格を支払うための自動決済を行う際に、無線識別子発信装置の前記固有の識別子を読取るための識別子送信要求があった場合に、匿名用偽識別子が匿名用偽識別子記憶手段から読出されて発信されるために、自動決済を行なうことができながらも、識別子を手がかりに、どの匿名ユーザがどの通常の個人ユーザか見破られてしまう不都合を極力防止できる。

【０４６０】

（２２）　前記匿名用偽識別子記憶手段は、複数の前記業者（たとえば、ＡＢＣ、ＭＴＴ、ＭＥＣ等）に対応してそれぞれ異なった匿名用偽識別子（たとえば、ａｂｃ、ｍｔｔ、ｍｅｃ等）を記憶しており（図９参照）、

前記発信手段は、前記複数の業者のうちのいずれに個人ユーザが匿名を名乗るかに応じて、当該匿名を名乗る業者に対応する前記匿名用偽識別子を前記匿名用偽識別子記憶手段から選択して発信する（図２９のＳＧ１１、ＳＧ１２等）ことを特徴とする、（１９）～（２１）のいずれかに記載のプライバシー保護用識別子発信装置。

【０４６１】

このような構成によれば、匿名用偽識別子記憶手段は、複数の前記業者に対応してそれぞれ異なった匿名用偽識別子を記憶しており、発信手段は、複数の業者のうちのいずれに個人ユーザが匿名を名乗るかに応じて、当該匿名を名乗る業者に対応する匿名用偽識別子を匿名用偽識別子記憶手段から選択して発信するために、業社毎に異なった匿名用識別子を使分けることができる。

【０４６２】

（２３）　固有の識別子（ＲＦＩＤ等）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプログラムであって、

プライバシー保護用識別子発信装置セキュリティ用のＲＦＩＤタグ１ａまたはブラウザフォン３０等）に設けられているコンピュータ（ロジック１００、ＲＯＭ１０１、ＲＡＭ１０２、ＥＥＰＲＯＭ１０３、またはＬＳＩチップ２０等）に、

プライバシー保護用の偽識別子を生成する手段であって、前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子生成手段（図１１のＳＡ１～ＳＡ４、または、図２６のＳＤ２、ＳＤ１０、ＳＤ１２と図２７のＳＥ１～ＳＥ１０と図２９のＳＧ３、ＳＧ３ａ、ＳＧ３ｂ、ＳＧ５～ＳＧ９、図５６、図５７等）と、

識別子の送信要求があった場合に（図１１のＳＡ１または図２９のＳＧ３によりＹＥＳの判断があった場合に）、前記可変型偽識別子生成手段により生成された偽識別子を発信する発信手段（図１１のＳＡ５、ＳＡ１０、またはＳＧ７、ＳＧ９等）と、

して機能させるための、プログラム。

【０４６３】

このような構成によれば、識別子の送信要求があった場合に、個人ユーザに所持されるプライバシー保護用識別子発信装置により偽識別子を生成して発信でき、しかも前回発信した偽識別子とは異なる偽識別子を生成可能な可変型偽識別子の生成ができるために、複数箇所に設置された無線識別子リーダ等のそれぞれにより同一人物から発せられる偽識別子が読取られたとしても、それぞれの無線識別子リーダ等には異なった偽識別子が読取られる状態にすることができ、同一人物であることをカムフラージュできてプライバシーの侵害を極力防止することができる。

【０４６４】

（２４）　前記可変型偽識別子生成手段は、既に販売済みとなっている商品それぞれに付された無線識別子発信装置（ＲＦＩＤタグ等）の各々が発信する識別子の範囲内で前記偽識別子を生成させることを特徴とする、（２３）に記載のプログラム。

【０４６５】

このような構成によれば、既に販売済みとなっている商品それぞれに付された無線識別

子発信装置の各々が発信する識別子の範囲内で可変型の偽識別子が生成されて発信されるために、発信された偽識別子が既に消費者の購入済み商品に付された無線識別子発信装置から発信される識別子と区別することができず、発信された識別子が偽の識別子であると見破られてしまう不都合を極力防止することができる。

【０４６６】

（２５）　前記発信手段は、前回の偽識別子の発信から所定時間内（たとえば５秒内）に再度識別子の送信要求があった場合に、前回発信した偽識別子と同じ偽識別子を発信させる（図１１のＳＡ２、ＳＡ１０、または図２９のＳＧ３ａ、ＳＧ３ｂ等）ことを特徴とする、（２３）または（２４）に記載のプログラム。

【０４６７】

このような構成によれば、発信手段が、前回の識別子の発信から所定時間内に再度識別子の送信要求があった場合に前回発信した識別子と同じ識別子を発信するために、識別子読取装置側における読取り制度の信頼性の向上等のために複数回連続して識別子の発信要求を送信して連続して複数回識別子を読取る方式が採用されたとしても、同じ偽識別子が発信されるために、連続して複数回読取られた識別子が異なることによる不都合を極力防止することができる。また、可変型の偽識別子であるかまたは本物の無線識別子発信装置から発信された固有の識別子であるかをチェックすることを目的として、前述と同様に複数回連続して識別し発信要求を送信して連続的に識別子を読取ることが行われたとしても、可変型の偽識別子であることが見破られてしまう不都合を極力防止することができる。

【０４６８】

（２６）　前記可変型偽識別子生成手段は、当該可変型偽識別子生成手段により偽識別子を生成するプライバシー保護用識別子発信装置を所持する人物とは異なった人物が所持するプライバシー保護用識別子発信装置から発信される識別子と互いに一致する共通の偽識別子を生成可能（図１２のＲが０～３９の領域に属する列のＲＦＩＤを生成可能、または図２７や図５６や図５７のＲＦＩＤ交換処理で互いに交換した偽ＲＦＩＤを生成可能）にすることを特徴とする、（２３）～（２５）のいずれかに記載のプログラム。

【０４６９】

このような構成によれば、それぞれ異なった人物に所持されたプライバシー保護用識別子発信装置から発信される可変型の偽識別子には、互いに一致する共通の偽識別子が含まれるように構成されている。その結果、異なった人物から発信された識別子でありながら前記共通の識別子即ち互いに一致する識別子が発信される現象（異人物同一識別子発信現象）を生じさせることができる。このような異人物同一識別子発信現象を生じさせることのできるプライバシー保護用識別子発信装置が個人ユーザの間に普及すれば、或る地点で読取った識別子と他の地点で読取った識別子とが一致することにより同一人物であると判定して当該同一人物の個人情報を不当に収集して悪用しようとする悪意のプライバシー侵害者にとってみれば、同一の識別子を受信すればその同一識別子の発信元は同一人物であるという判定の信頼性が持てなくなる。よって、同一人物であるとの判定に基づいたプライバシー侵害行為を前提から覆すことができ、個人ユーザのプライバシーを有効に保護することが可能となる。

【０４７０】

しかも、大多数の個人ユーザが購入済み商品に付されている無線識別子発信装置から固有の識別子を発信する状態にしたままそれを所持して屋外等を歩いたとしても、一部のユーザの間でこの共通の偽識別子を発信できるプライバシー保護用識別子発信装置が普及することにより、同一人物の所持品に付された無線識別子発信装置から発信された同一の識別子が悪意のプライバシー侵害者側に複数箇所で読取られたとしても、それが同一人物であるとの信頼性を低下させることができるという撹乱効果を期待でき、このプライバシー保護用識別子発信装置を所持していない個人ユーザのプライバシーをも極力保護することが可能となる。

【０４７１】

（２７）　前記可変型偽識別子生成手段は、識別子を記憶する識別子記憶手段（図２７

、図５６、図５７のＳＥ９、ＳＥ１０とＥＥＰＲＯＭ１９４等）を含み、
前記他のプライバシー保護用識別子発信装置と交信して（図２７の直接電波交信、図５６の通話交信、図５７の電子メール交信等）、前記識別子記憶手段に記憶している前記識別子を前記他のプライバシー保護用識別子発信装置に送信させるとともに（図２７のＳＥ６、ＳＥ８、または図５６のＳＳ８、ＳＥ９、ＳＥ１０、または図５７のＳＥ６、ＳＴ３等）当該他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させて（図２７のＳＥ７～ＳＥ１０、または図５６のＳＥ７、ＳＳ８、または図５７のＳＴ８、ＳＥ９、ＳＥ１０等）、記憶している互いの識別子を交換し、
前記可変型偽識別子生成手段は、識別子の送信要求があった場合に（図２９のＳＧ３によりＹＥＳの判断があった場合に）、前記識別子記憶手段に記憶している交換後の識別子を読出すことにより前記共通の偽識別子として生成させる（図２９のＳＧ９等）ことを特徴とする、（２６）に記載のプログラム。

【０４７２】

このような構成によれば、プライバシー保護用識別子発信装置同士で交信して、互いに記憶している識別子同士を送受信して互いの識別子を交換する。そして、識別子の送信要求があった場合には、前述した交換後の識別子が前述の共通の偽識別子として生成されて発信される。その結果、互いに交信して識別しを交換するという比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

【０４７３】

（２８）　既に交信して前記識別子の交換を行なった他のプライバシー保護用識別子発信装置と所定期間内（たとえば１日以内）に再度前記識別子の交換を行なうことを禁止する禁止手段（図２７図、図５６、図５７のＳＥ３等）として機能させることを特徴とする、（２６）または（２７）に記載のプログラム。

【０４７４】

このような構成によれば、既に交信して識別子の交換を行なった他のプライバシー保護用識別子発信装置と所定期間内に再度識別子の交換を行なうことを防止でき、既に識別子交換済みの相手と所定期間内に再度識別子の交換を行なうという無駄を防止することができる。

【０４７５】

（２９）　電話（ブラウザフォン３０による通話）で交信した他のプライバシー保護用識別子発信装置と互いの識別子を交換し（図５６のＲＦＩＤ交換処理等）、
前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している交換後の識別子を読出すことにより前記共通の偽識別子として生成させる（図２９のＳＧ９）ことを特徴とする、（２６）～（２８）のいずれかに記載のプログラム。

【０４７６】

このような構成によれば、交信手段が電話機能を有しており、電話で交信した他のプライバシー保護用識別子発信装置と互いの識別子の交換を行なうために、比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

【０４７７】

（３０）　電子メール（ブラウザフォン３０によるＥメール）の送信とともに前記識別子記憶手段に記憶している識別子を他のプライバシー保護用識別子発信装置に送信し（図５７のＳＥ５、ＳＥ６、ＳＴ３等）、電子メールの受信とともに他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して前記識別子記憶手段に記憶させ（図５７のＳＴ８、ＳＥ９、ＳＥ１０等）、
前記可変型偽識別子生成手段は、識別子の送信要求があった場合に、前記識別子記憶手段に記憶している他のプライバシー保護用識別子発信装置から送信されてきた識別子を読

出すことにより前記共通の偽識別子として生成させる（図２９のＳＧ９）ことを特徴とする、（２６）～（２９）のいずれかに記載のプライバシー保護用識別子発信装置。

【０４７８】

このような構成によれば、交信手段が電子メール機能を有しており、電子メールの送信とともに識別子記憶手段に記憶している識別子を他のプライバシー保護用識別子発信装置に送信し、電子メールの受信とともに他のプライバシー保護用識別子発信装置から送信されてきた識別子を受信して識別子記憶手段に記憶させることにより互いの識別子の交換を行なうために、比較的確実な方法で共通の偽識別子を生成し発信して前述の異人物同一識別子発信現象を生じさせることができる。

【０４７９】

（３１）　前記発信手段は、他のプライバシー保護用識別子発信装置（図１２（ａ）のテーブルを記憶しているＲＦＩＤタグ１ａ等）から１度に発信される所定個数たとえば１個）の偽識別子よりも多い複数の偽識別子を１度に発信させることが可能であり図１２（ｂ）（ｃ）の４個のＲＦＩＤ１～４、図１１のＡＳ４、ＡＳ５等）、

前記可変型偽識別子生成手段は、前記複数の偽識別子のうちの前記所定個数を除く他の偽識別子を前記共通の偽識別子として生成させる（図１２（ａ）（ｃ）のＲＦＩＤ２～４を共通の偽ＲＦＩＤとして生成する）ことを特徴とする、（２３）～（３０）のいずれかに記載のプログラム。

【０４８０】

このような構成によれば、或る個人ユーザに提供されたプライバシー保護用識別子発信装置から予め定められた所定個数の偽識別子が１度に発信される一方、前記或る個人ユーザとは異なる他の個人ユーザに提供されたプライバシー保護用識別子発信装置から前記所定個数よりも多い複数の偽識別子が一度に発信され、その複数の偽識別子の内の前記所定個数を除く他の偽識別子が前記共通の偽識別子として生成されて発信される。その結果、個人ユーザに所持された購入済物品から他人が固有の識別子を読取ることのできる状態になっていたとしても、前述の異人物同一識別子発信現象を生じさせることができる。

【０４８１】

つまり、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザが偽識別子を発信するプライバシー保護用識別子発信装置を所持した場合には、購入済の所持品に付されている無線識別子発信装置とプライバシー保護用識別子発信装置との両方から識別子が発信されることとなり、１度に複数の識別子が発信される状態となる。そして、その複数の識別子中の一部が可変型であり他の一部が変化しない固定型となる。つまり、複数箇所で識別子が読取られた時にはそれぞれに読取られた複数の識別子中の所定個数のもののみが可変型の異なった偽識別子となりその他のものは携帯品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象（複数識別子中所定個数可変型現象）が生ずる。その結果、この複数識別子中所定個数可変型現象が生じれば同一人物であることが見破られてしまう不都合が生じる。

【０４８２】

そこで本発明では、たとえば、購入済の所持品に付されている無線識別子発信装置から固有の識別子が発信される状態になっている個人ユーザに前記所定個数の偽識別子を一度に発信する少数識別子発信タイプのプライバシー保護用識別子発信装置を提供し、購入済の所持品から固有の識別子が他人に読取られない状態になっている個人ユーザに対し前記所定個数よりも多い複数の偽識別子を一度に発信する多数識別子発信タイプのプライバシー保護用識別子発信装置を提供する。その結果、前者の個人ユーザからは、所定個数の偽識別子と購入済所持品の無線識別子発信装置から発信される固有の識別子とが同時に発信される一方、後者の個人ユーザからは、前者の個人ユーザが発信される偽識別子よりも多い偽識別子が一度に発信され、その多い偽識別子の内前者の個人ユーザから発信される偽識別子の個数（所定個数）を除く他の偽識別子が前述の共通の偽識別子として生成されて発信されることとなる。これにより、前者の個人ユーザの場合には、複数箇所で識別子が

読取られた時にはそれぞれに読取られた複数の識別子中の前記所定個数のもののみが可変型の異なった偽識別子となりその他のものは所持品に付されている無線識別子発信装置から発信された本物の固有識別子となり同一の識別子となる現象（複数識別子中所定個数可変型現象）が生ずる。一方、多数識別子発信タイプのプライバシー保護用識別子発信装置を所持する後者のユーザ同士の間では、複数発信された偽識別子の内前記所定個数を除く他の偽識別子が前述の共通の偽識別子として生成されて発信可能であるために、やはり複数識別子中所定個数可変型現象が生ずる。しかもこの現象は、異なった人物の間で生ずる。

【０４８３】

以上より、前述の複数識別子中所定個数可変型現象が生じたとしてもそれが必ずしも同一人物で生ずるとは限らず、異なった人物の間でも生ずる現象となり、悪意のプライバシー侵害者による複数識別子中所定個数可変型現象に基づく同一人物であるとの推測の信頼性を低下させることができる。

【０４８４】

（３２）　購入されることにより個人ユーザの所持品となった物品（たとえば、腕時計、眼鏡、衣服等）に付されている無線識別子発信装置（ＲＦＩＤタグ等）の固有の識別子（ＲＦＩＤ等）を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガード手段（図１５のＳＢ１、ＳＢ３～ＳＢ７等）と、

識別子ガード状態となっている前記無線識別子発信装置の識別子を、個人ユーザの意思に従って読取ることができるようにする読取り手段（図１５のＳＢ２、ＳＢ８、ＳＢ９～ＳＢ１３）と、

して機能させるプログラムをさらに含むことを特徴とする、（２３）～（３１）のいずれかに記載のプログラム。

【０４８５】

このような構成によれば、購入されることにより個人ユーザの所持品となった物品に付されている無線識別子発信装置の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にすることができ、購入済みの物品に付されている無線識別子発信装置の固有の識別子を他人により読取られてそれに基づくプライバシーの侵害が発生する不都合を極力防止することができる。しかも識別子ガード状態となっている無線識別子発信装置の識別子を 個人ユーザの意思に従って読取ることができるようにするために、購入済みの物品に付されている無線識別子発信装置の固有の識別子を利用したサービスを個人ユーザが受けたいと思う必要なときに読取ってサービスを享受することが可能となる。

【０４８６】

（３３）　前記識別子ガード手段は、本人認証のための固有識別情報（たとえばパスワード）を発信して前記無線識別子発信装置に認証させて本人確認ができない限り識別子を発信しない識別子発信停止状態に切換え（図１５のＳＢ３～ＳＢ８等）、

前記読取り手段は、前記固有識別情報を発信して前記無線識別子発信装置に本人認証を行なわせた上で識別子を発信可能状態にさせる（図１５のＳＢ８、ＳＢ９～ＳＢ１３等）ことを特徴とする、（３２）に記載のプログラム。

【０４８７】

このような構成によれば、識別子ガード手段により、本人認証のための固有識別情報を発信して前記無線識別子発信装置に認証させて本人確認ができない限り識別子を発信しない識別子発信停止状態に切換え、読取り手段により、固有識別情報を発信して無線識別子発信装置に本人認証を行なわせた上で識別子を発信可能状態にするために、確実に無線識別子発信装置の識別子をガードした状態にできるとともに、本人認証が行われた本人のみが無線識別子発信装置を識別子発信可能状態にすることができ、セキュリティを向上させることができる。

【０４８８】

[構成と実施形態との対応関係]

次に、本発明の構成と実施の形態との対応関係を、本発明の構成中に実施の形態の開示内容を括弧書き挿入して示す。

【０４８９】

（１）　個人ユーザに関する固有の識別子（たとえば、ＲＦＩＤ）が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を監視するためのプライバシー保護方法であって、

購入されることにより個人ユーザの所持品となった物品（たとえば、眼鏡、衣服、腕時計等）に付されている無線識別子発信装置（たとえば、ＲＦＩＤタグ）の固有の識別子を、当該個人ユーザの意思に従って他人が読取れない識別子ガード状態にする識別子ガードステップ（たとえば、図１５のＳＢ１～ＳＢ８）と、

前記個人ユーザが顧客またはユーザとして所定の業者（たとえば、ＭＴＴ、百貨店２０６等）に自己のメールアドレスを通知するときに、当該業社用としての新たな通知用メールアドレスであって当該業社を特定する情報を割出すことができる通知用メールアドレス（たとえば、図６１の#ｅ９¥８２%３１＆０αｔ＊ｃ）を生成して当該業社に通知するための処理を行うメールアドレス通知処理ステップ（たとえば、図５９のＳＵ１～ＳＵ７、Ｓ１０００～Ｓ１００３）と、

前記メールアドレス通知処理ステップにより前記通知用メールアドレスを通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成ステップ（たとえば、図３５のＳ２７３～Ｓ２７９）と、

識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成ステップにより生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信ステップ（たとえば、図２８のＳＦ７ａ、ＳＦ７ｂ、図２９のＳＧ４、ＳＧ１０～ＳＧ１３）と、

送信元から送信された電子メールを指定されたメールアドレスに従って送信先に送信するための電子メール送信ステップ（たとえば、図２０のＳ５１４～Ｓ５２１または図６０のＳＶ２、ＳＶ５～ＳＶ１６）と、

該電子メール送信ステップにより送信される電子メールの送信先のメールアドレスが、前記メールアドレス通知処理ステップにより通知した前記通知用メールアドレスである場合に、当該通知用メールアドレスに対応する前記通知業社を特定する情報を割出し、該割出された通知業社を特定する情報と当該電子メールの送信元の情報とが一致するか否か監視する監視ステップ（たとえば、図６０のＳＶ５～ＳＶ１２）とを含むことを特徴とする、プライバシー保護方法。

【０４９０】

（２）　個人ユーザに関する固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護システムであって、

前記個人ユーザが顧客またはユーザとして所定の業者（たとえば、ＭＴＴ、百貨店２０６等）に自己のメールアドレスを通知するときに、当該業社用としての新たな通知用メールアドレスであって当該業社を特定する情報を割出すことができる通知用メールアドレス（たとえば、図６１の#ｅ９¥８２%３１＆０αｔ＊ｃ）を生成して当該業社に通知するための処理を行うメールアドレス通知処理手段（たとえば、図５９のＳＵ１～ＳＵ７、Ｓ１０００～Ｓ１００３）と、

前記メールアドレス通知処理手段により前記通知用メールアドレスを通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成手段（たとえば、図３５のＳ２７３～Ｓ２７９）と、

識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成手段により生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信

手段（たとえば、図２８のＳＦ７ａ、ＳＦ７ｂ、図２９のＳＧ４、ＳＧ１０～ＳＧ１３）と、

送信元から送信された電子メールの送信先のメールアドレスが、前記メールアドレス通知処理手段により通知した前記通知用メールアドレスである場合に、当該通知用メールアドレスに対応する前記通知業社を特定する情報を割出し、該割出された通知業社を特定する情報と当該電子メールの送信元の情報とが一致するか否か監視する監視手段（たとえば、図６０のＳＶ５～ＳＶ１２）とを含むことを特徴とする、プライバシー保護システム。

【０４９１】

（３）　前記メールアドレス通知処理手段は、メールアドレスを通知する通知業社を特定するための通知業社特定情報を含むデータを暗号化して前記通知用メールアドレスを生成する暗号化生成手段（たとえば、図５９のＳ１００１、Ｓ１００２）を含み、

前記監視手段は、

送信元から送信された電子メールの通知用メールアドレスを復号する復号手段（たとえば、図６０のＳＶ５～ＳＶ７）と、

該復号手段により復号されたデータ中に含まれている前記通知業社特定情報と当該電子メールの送信元の情報とが一致するか否かを判定する判定手段（たとえば、図６０のＳＶ８～ＳＶ１２）とを含むことを特徴する、請求項２に記載のプライバシー保護システム。

【０４９２】

（４）　前記通知業者は、商品を販売する販売店（たとえば、百貨店２０６）であり、

前記メールアドレス通知処理手段は、前記販売店においてポイントカードの発行に伴うユーザ登録の際に当該販売店に対応する通知用メールアドレスを生成して通知する処理を行い（たとえば、図３２のＳＪ１～ＳＪ９）、

前記発信手段は、前記販売店において購入する商品に付されている無線識別子発信装置から発信される固有の識別子を利用して割出される当該商品の販売価格に従って自動決済を行う際に（たとえば、）、前記無線識別子発信装置の前記固有の識別子を読取るための識別子送信要求があった場合に（たとえば、図３１の自動決済処理による自動決済時に）、前記販売店に対応する前記通知業者用識別子を発信する（たとえば、図３１のＳＨ２により受信した販売業者の店名信号に応じて図２９のＳＧ１０→ＳＧ１１→ＳＧ１２と進み、受信した業社に対応するトラップ型ＲＦＩＤを発信する）ことを特徴とする、請求項２または請求項３に記載のプライバシー保護システム。

【０４９３】

（５）　個人ユーザに関する固有の識別子が読取られて該固有の識別子に基づいて行われるプライバシーの侵害を防止するためのプライバシー保護用識別子発信装置であって、

前記個人ユーザが顧客またはユーザとなった所定の業者のために新たな通知用メールアドレスを生成して当該業社に通知した通知業者に対応した通知業者用識別子を生成する通知業者用識別子生成手段（たとえば、図３５のＳ２７３～Ｓ２７９）と、

識別子の送信要求に応じて、前記通知業者に対し識別子を発信する場合には、前記通知業者用識別子生成手段により生成された毎回同じ前記通知業社用識別子を発信し、かつ、前記通知業者以外の者に対し識別子を発信する場合であっても、前記通知業者用識別子を発信する旨の個人ユーザの操作があった場合には、前記通知業者用識別子を発信する発信手段（たとえば、図２８のＳＦ７ａ、ＳＦ７ｂ、図２９のＳＧ４、ＳＧ１０～ＳＧ１３）とを含むことを特徴とする、プライバシー保護用識別子発信装置。

【０４９４】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【０４９５】

【図１】プライバシー保護システムの全体構成を示す概略システム図である。
【図２】金融機関に設置されたデータベースに記憶されている各種データを示す説明図である。
【図３】金融機関に設置されたデータベースに記憶されている各種データを示す説明図である。
【図４】金融機関に設置されているデータベースに記憶されている各種データを示す説明図である。
【図５】ＸＭＬストアのデータベースに記憶されている各種データを示す説明図である。
【図６】コンビニエンスストアに設置されているデータベースに記憶されている各種情報を説明するための説明図である。
【図７】ユーザ端末の一例としてのブラウザフォンを示す正面図である。
【図８】ユーザ端末の一例としてのブラウザフォンを示す正面図である。
【図９】ＶＰ用ＩＣ端末のトラップ型ＲＦＩＤ記憶領域に記憶されているトラップ型ＲＦＩＤデータの内訳を示す図である。
【図１０】セキュリティ用のＲＦＩＤタグおよびその回路ブロック図
【図１１】セキュリティ用のＲＦＩＤタグの制御プログラムを示すフローチャート
【図１２】セキュリティ用のＲＦＩＤタグに記憶されているテーブル
【図１３】セキュリティ用のＲＦＩＤタグの地域を指定しての販売の方法を説明する説明図
【図１４】ブラウザフォンの制御プログラムを示すフローチャート
【図１５】ＲＦＩＤタグ切換え処理のサブルーチンプログラムを示すフローチャート
【図１６】購入商品に付されているＲＦＩＤタグの制御プログラムを示すフロータート
【図１７】ＶＰ管理サーバの処理動作を示すフローチャート
【図１８】（ａ）はＶＰ管理サーバの処理動作を示すフローチャートであり、（ｂ）は個人情報の登録処理のサブルーチンプログラムを示すフローチャート
【図１９】トラップ情報の登録処理のサブルーチンプログラムを示すフローチャート
【図２０】メール転送，流通チェックのサブルーチンプログラムを示すフローチャート
【図２１】認証用サーバの処理動作を示すフローチャート
【図２２】決済サーバの処理動作を示すフローチャート
【図２３】決済サーバの処理動作を示すフローチャート
【図２４】（ａ）は決済処理のサブルーチンの一部、（ｂ）は正当機関証明処理のサブルーチンプログラムを示すフローチャート
【図２５】クレジットカード発行会社からの問合せ処理のサブルーチンプログラムを示すフローチャート
【図２６】ブラウザフォンの偽モード処理のサブルーチンプログラムを示すフローチャート
【図２７】ブラウザフォンのＲＦＩＤ交換処理のサブルーチンプログラムを示すフローチャート
【図２８】ブラウザフォンのトラップモード処理のサブルーチンプログラムを示すフローチャート
【図２９】ブラウザフォンのＲＦＩＤ発信処理のサブルーチンプログラムを示すフローチャート
【図３０】ＲＦＩＤタグを利用した百貨店での自動決済の説明図
【図３１】ブラウザフォンの自動決済処理のサブルーチンプログラムを示すフローチャート
【図３２】（ａ）はブラウザフォンのポイントカード加算処理のサブルーチンプログラムを示すフローチャート、（ｂ）はブラウザフォンのポイントカード登録処理のサ

ブルーチンプログラムを示すフローチャート
【図３３】販売業者決済サーバの制御用プログラムを示すフローチャート
【図３４】ＶＰ用ＩＣ端末の処理動作を示すフローチャート
【図３５】（ａ）は暗証番号チェック処理のサブルーチンプログラムを示すフローチャートであり、（ｂ）はトラップ型ＲＦＩＤ処理のサブルーチンプログラムを示すフローチャートであり、（ｃ）は本人証明処理（ＶＰ用）のサブルーチンプログラムを示すフローチャートである。
【図３６】（ａ）はデータ入力処理のサブルーチンプログラムを示すフローチャートであり、（ｂ）はユーザエージェント動作処理のサブルーチンプログラムを示すフローチャートであり、（ｃ）はリロード金額の使用処理のサブルーチンプログラムを示すフローチャートであり、（ｄ）はＶＰ署名処理のサブルーチンプログラムを示すフローチャートである。
【図３７】トラップ型ＶＰ処理のサブルーチンプログラムを示すフローチャートである。
【図３８】コンビニサーバの処理動作を示すフローチャートである。
【図３９】コンビニサーバの処理動作を示すフローチャートであり、（ａ）は暗証番号チェック処理のサブルーチンプログラムを示すフローチャートであり、（ｂ）は本人チェック処理のサブルーチンプログラムを示すフローチャートであり、（ｃ）は決済処理のサブルーチンプログラムを示すフローチャートである。
【図４０】（ａ）は、ＶＰ用ＩＣ端末に記憶されているトラップ情報であり、（ｂ）は、トラップ型ＶＰ処理のサブルーチンプログラムを示すフローチャートであり、（ｃ）は、ＶＰ用ＩＣ端末の制御動作を示すフローチャートである。
【図４１】商品情報提供サービスシステムの全体概略を示す構成図である。
【図４２】商品情報サービス業者のＷｅｂデータベースに記憶されている商品ホームページを示す説明図である。
【図４３】商品情報サービス業者のＷｅｂサーバの制御用プログラムを示すフローチャートの一部である。
【図４４】商品情報サービス業者のＷｅｂサーバの制御用プログラムを示すフローチャートの一部である。
【図４５】ブラウザフォンの商品検索・購入処理のサブルーチンプログラムを示すフローチャートの一部である。
【図４６】ブラウザフォンの商品検索・購入処理のサブルーチンプログラムを示すフローチャートの一部である。
【図４７】生産者のＷｅｂサーバの制御用プログラムを示すフローチャートである。
【図４８】住所，氏名，Ｅメールアドレスの送信処理のサブルーチンプログラムを示すフローチャートである。
【図４９】ＶＰ出生依頼処理のサブルーチンプログラムを示すフローチャートである。
【図５０】（ａ）は正当機関チェック処理のサブルーチンプログラムを示すフローチャートであり、（ｂ）は電子証明書発行要求処理のサブルーチンプログラムを示すフローチャートである。
【図５１】（ａ）はＶＰ用入力処理のサブルーチンプログラムを示すフローチャートであり、（ｂ）はＲＰ用入力処理のサブルーチンプログラムを示すフローチャートである。
【図５２】ＳＥＴによる決済処理の概要を説明するための説明図である。
【図５３】ＶＰ用決済処理のサブルーチンプログラムを示すフローチャートである。
【図５４】（ａ）は本人証明処理のサブルーチンプログラムを示すフローチャートであり、（ｂ）はＶＰ用決済処理のサブルーチンプログラムの一部を示すフローチャートである。
【図５５】ＶＰ用決済処理のサブルーチンプログラムの一部を示すフローチャートで

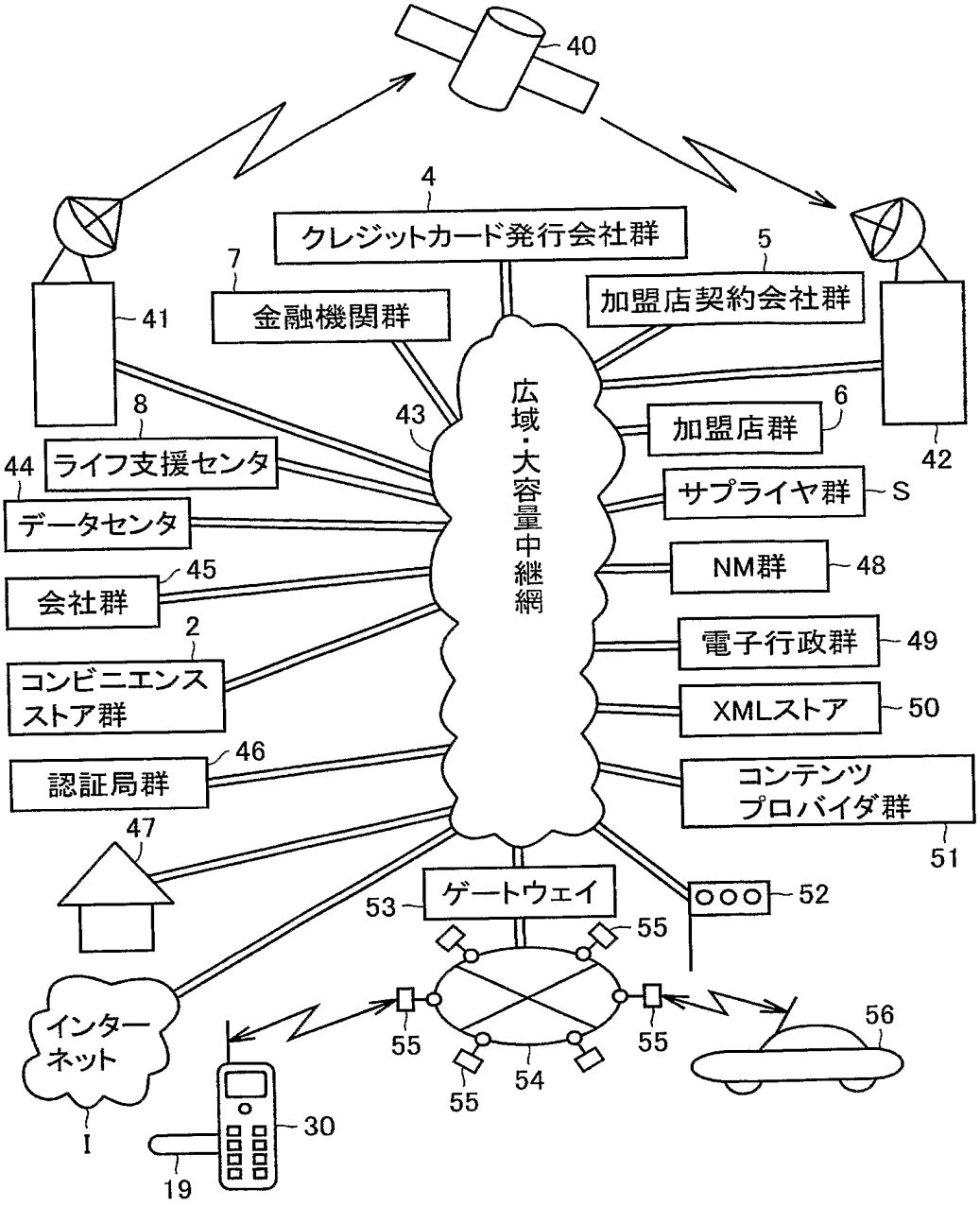
ある。
【図５６】別実施の形態におけるブラウザフォンのＲＦＩＤ交換処理のサブルーチンプログラムを示すフローチャートである。
【図５７】別実施の形態におけるブラウザフォンのＲＦＩＤ交換処理のサブルーチンプログラムを示すフローチャートである。
【図５８】メールサーバのデータベースに記憶されているデータを説明するための説明図である。
【図５９】（ａ）は、ブラウザフォンによるＥメールアドレス通知処理のサブルーチンプログラムを示すフローチャートであるり、（ｂ）は、ＩＣ端末によるＥメールアドレス生成処理のサブルーチンプログラムを示すフローチャートである。
【図６０】メールサーバの制御処理を示すフローチャートである。
【図６１】図５９、図６０に示した制御内容を分かり易く説明するための説明図である。

【符号の説明】

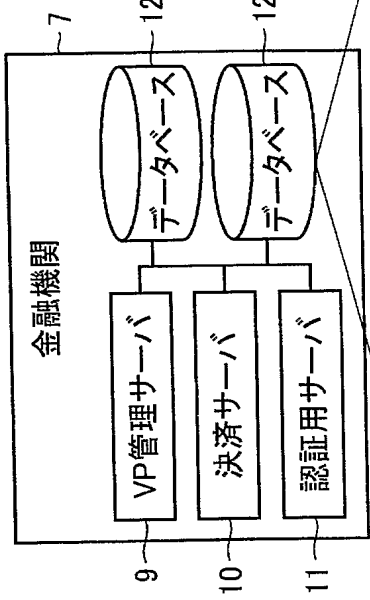
【０４９６】

３０　ブラウザフォン、７　金融機関、５０　ＸＭＬストア、１２ａ　データベース、２　コンビニエンスストア、１９Ｖ　ＶＰ用ＩＣ端末、２６　ＥＥＰＲＯＭ、１９４　ＥＥＰＲＯＭ、１　形態装置、１ａ　セキュリティ用のＲＦＩＤタグ、１１０　コンデンサ、２０６　決済用の通過ゲート、８０　メールサーバ、８２　業社側端末、８５　Ｅメール。

【書類名】図面
【図１】


40
4
クレジットカード発行会社群
5
加盟店契約会社群
7
金融機関群
41
42
広域・大容量中継網
8
43
6
加盟店群
44
ライフ支援センタ
サプライヤ群
S
データセンタ
45
会社群
NM群
48
2
コンビニエンスストア群
電子行政群
49
XMLストア
50
46
認証局群
コンテンツプロバイダ群
51
47
53
ゲートウェイ
52
55
インターネット
55
55
54
55
56
30
19
I

【図２】



RP					VP		
氏名	住所	認証鍵	公開鍵	口座番号	トラップ情報	個人情報	住所
太郎	○△×	KNT	KPT	8824	第1トラップ情報	第1個人情報	□×○
次郎	×○×	KNJ	KPJ	9017	第2トラップ情報	第2個人情報	△○○
					第3トラップ情報	第3個人情報	△○○
花子	○△○	KNH	KPH	2534	第4トラップ情報	第4個人情報	△×××
----	----	----	----	----	----	----	----

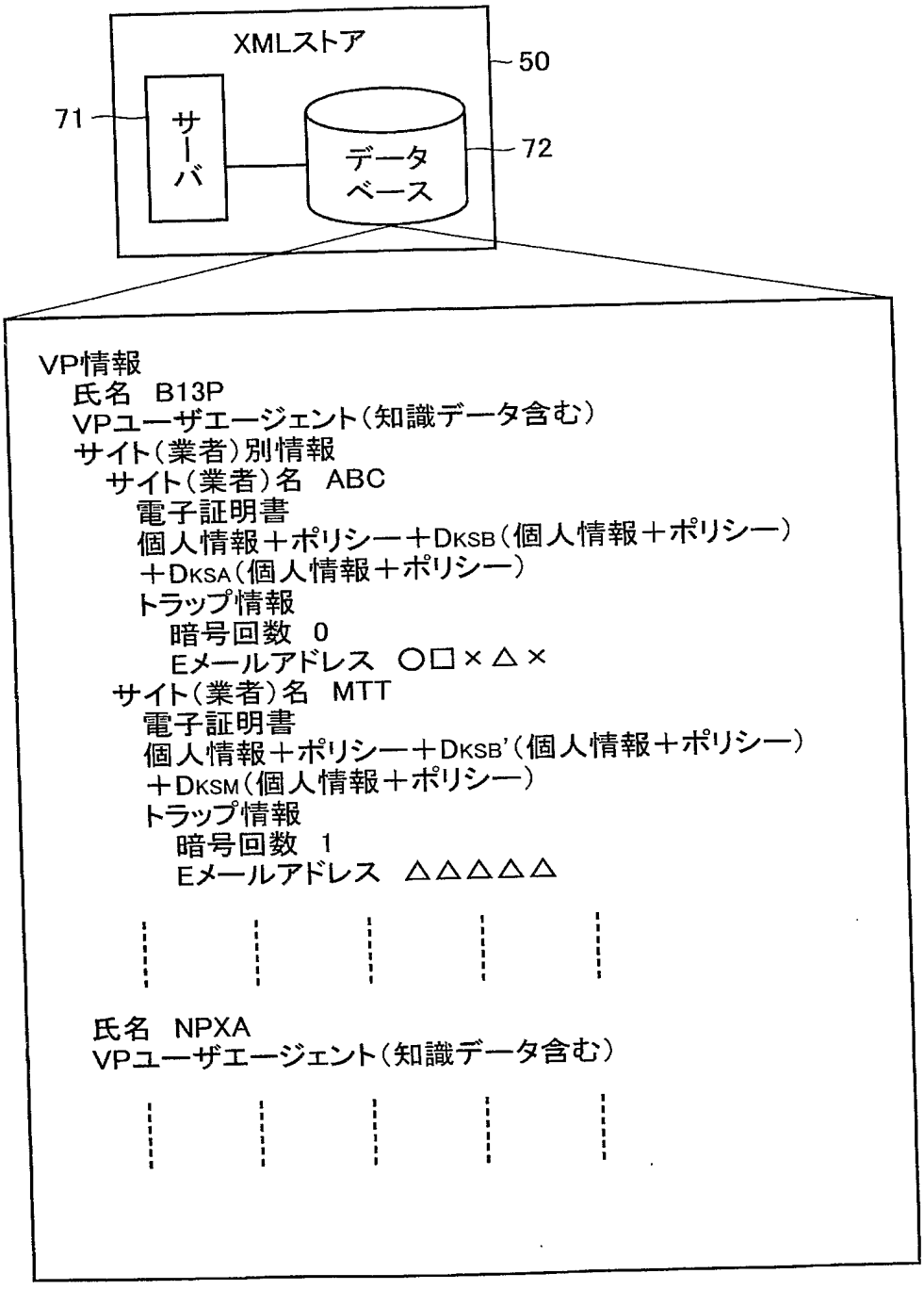
【図３】

第1トラップ情報	サイト名（業者名）	ABC	MTT	MEC	---------
	氏名	B13P	E(B13P)	E^2(B13P)	---------
	公開鍵	KPB	KPB'	KPB″	---------
	Eメールアドレス	○□×△×	△△△△△	△△△△△	---------
	バーチャル口座番号	2503	E(2503)	E^2(2503)	---------
	バーチャルクレジット番号	9145	E(9145)	E^2(9145)	---------
第2トラップ情報	サイト名（業者名）	AMZ	RAK	ASK	---------
	氏名	NPXA	E(NPXA)	E^2(NPXA)	---------
	公開鍵	KPN	KPN'	KPN″	---------
	Eメールアドレス	××○△□	△△△△△	△△△△△	---------
	バーチャル口座番号	3541	E(3541)	E^2(3541)	---------
	バーチャルクレジット番号	3288	E(3288)	E^2(3288)	---------
⋮	⋮	⋮	⋮	⋮	

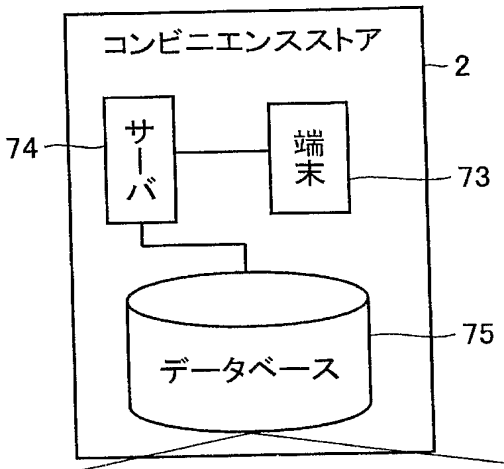
【図４】

	個人情報A	個人情報B	--------
第1個人情報	○○△＋DKS(○○△)	××△＋DKS(××△)	--------
第2個人情報	△○○＋DKS(△○○)	△××＋DKS(△××)	--------
第3個人情報	○△○＋DKS(○△○)	×△×＋DKS(×△×)	--------
第4個人情報	△○△＋DKS(△○△)	△×△＋DKS(△×△)	--------
⋮	⋮	⋮	

【図５】

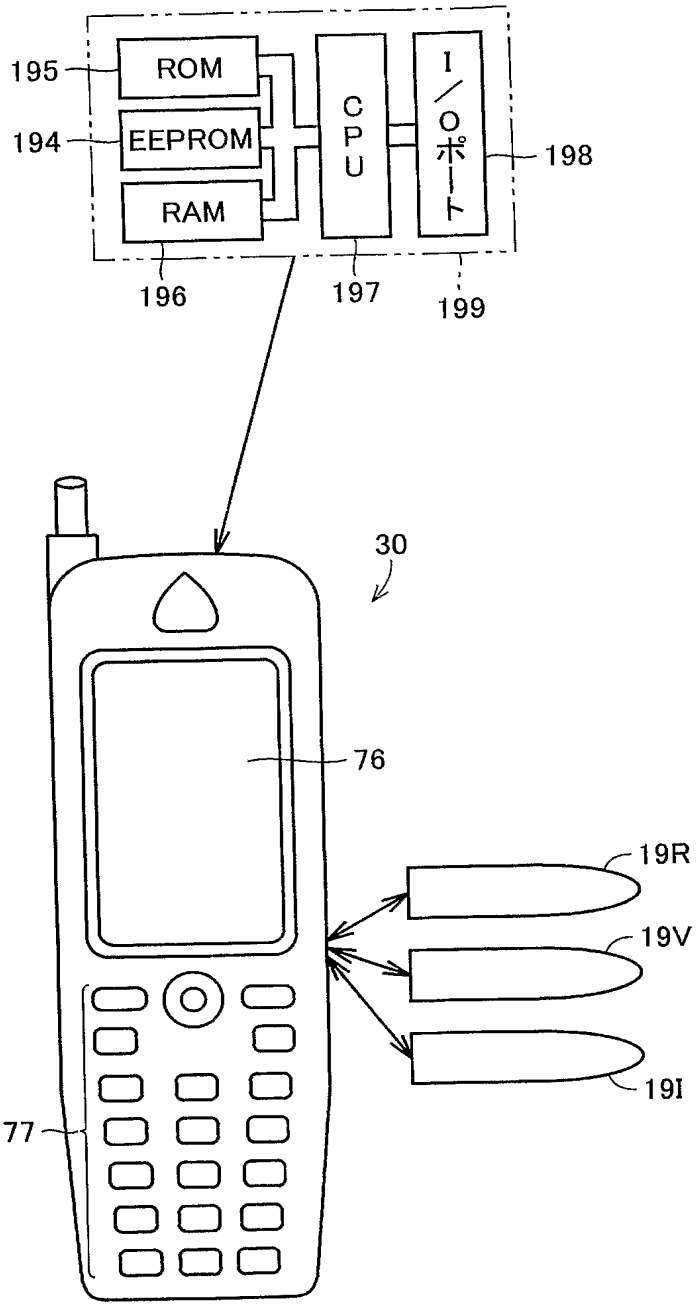

XMLストア
50
71
サーバ
データベース
72
VP情報
氏名　B13P
VPユーザエージェント(知識データ含む)
サイト(業者)別情報
サイト(業者)名　ABC
電子証明書
個人情報＋ポリシー＋DKSB(個人情報＋ポリシー)
＋DKSA(個人情報＋ポリシー)
トラップ情報
暗号回数　0
Eメールアドレス　○□×△×
サイト(業者)名　MTT
電子証明書
個人情報＋ポリシー＋DKSB'(個人情報＋ポリシー)
＋DKSM(個人情報＋ポリシー)
トラップ情報
暗号回数　1
Eメールアドレス　△△△△△
氏名　NPXA
VPユーザエージェント(知識データ含む)

【図６】

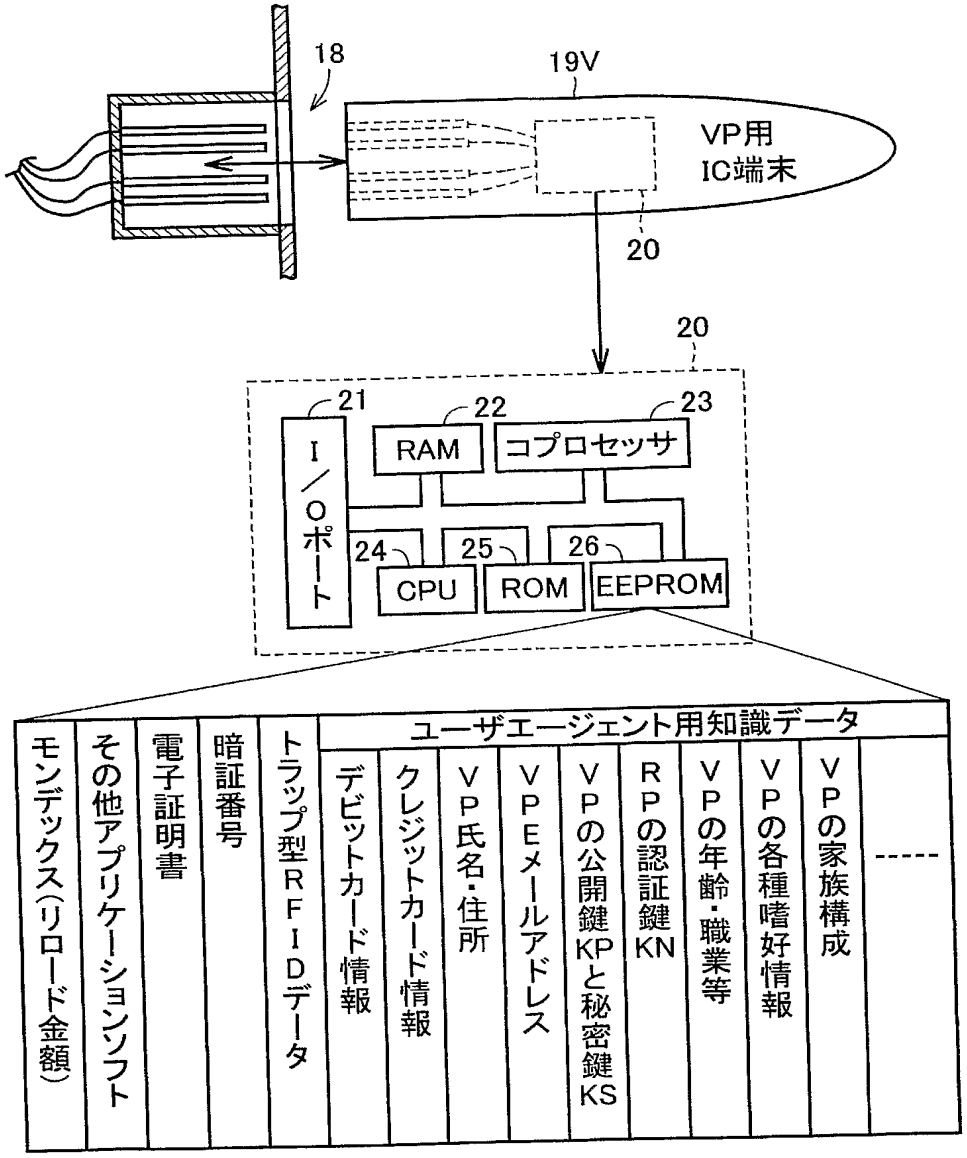


VP氏名	商品預かり情報	Eメールアドレス	顧客管理情報
B13P	ABC会社からの商品預かり，未決済	○□×△×	----------
E(B13P)	MTT会社からの商品預かり，決済済	△△△△△	----------
E^2(NPXA)	MEC会社からの商品預かり，未決済	△△△△△	----------
⋮	⋮	⋮	⋮

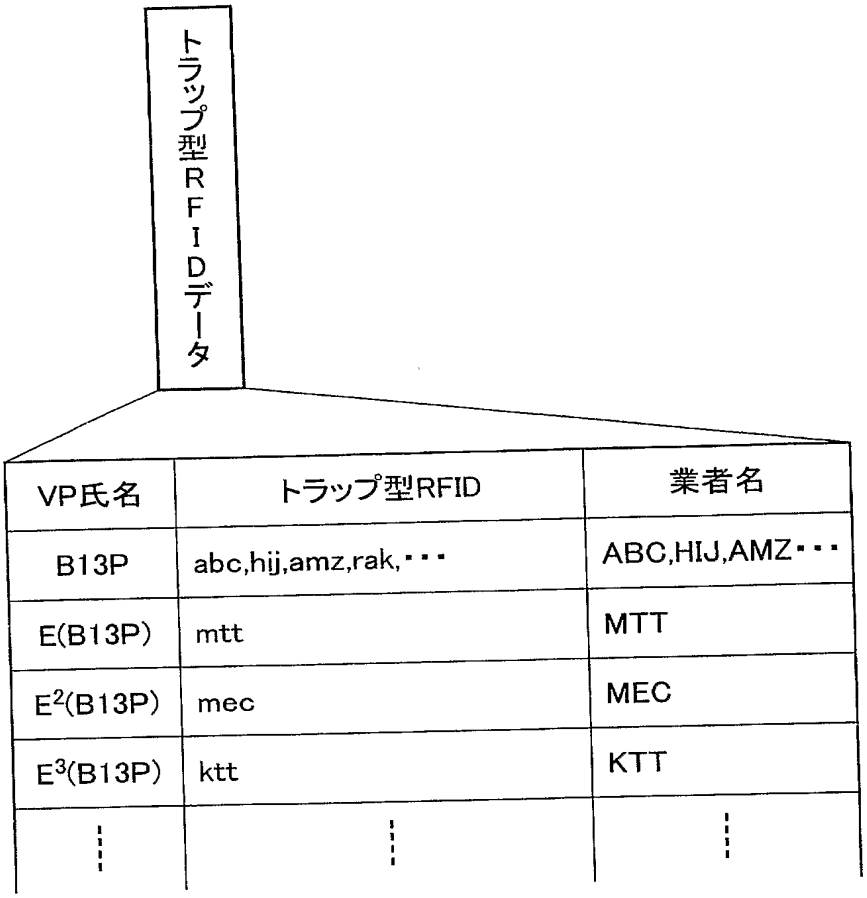
【図７】


195
ROM
194
EEPROM
RAM
CPU
I／Oポート
198
196
197
199
30
76
19R
19V
19I
77

【図８】

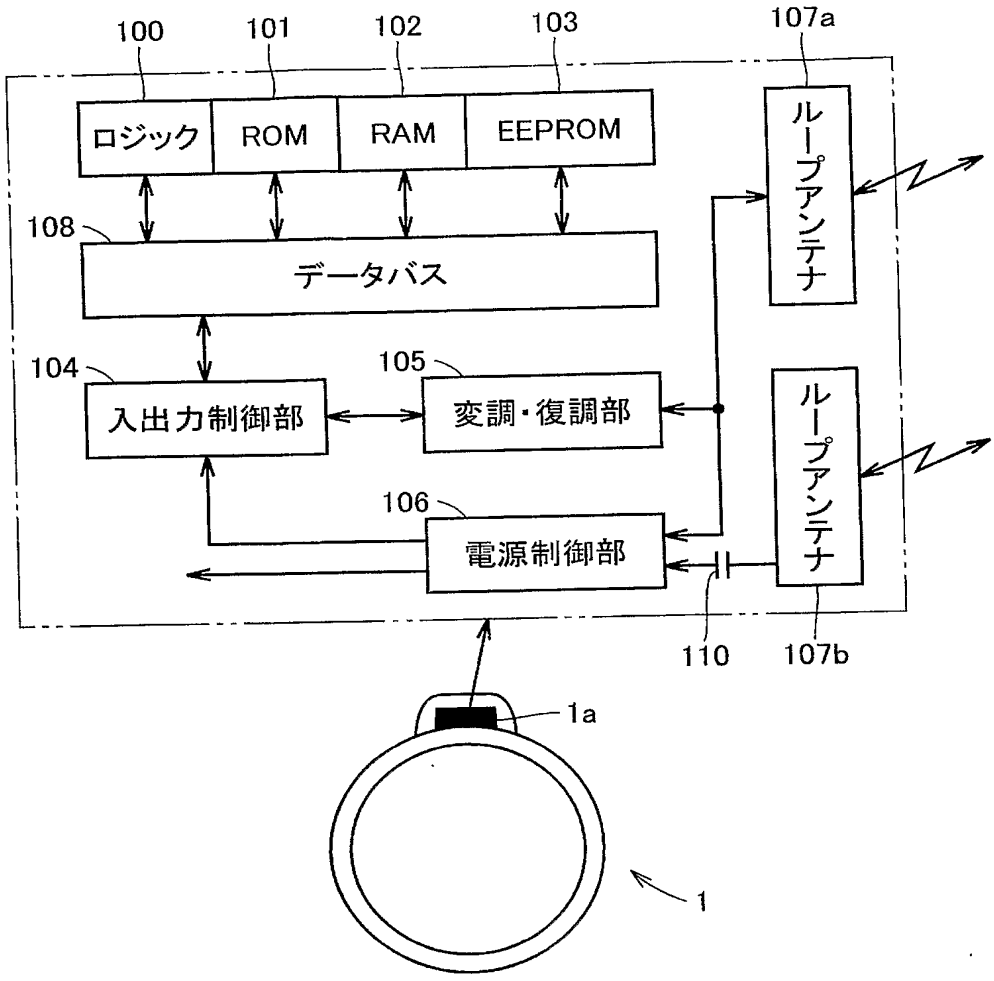

18
19V
VP用
IC端末
20
20
21
22
23
I／Oポート
RAM
コプロセッサ
24
25
26
CPU
ROM
EEPROM
ユーザエージェント用知識データ
トラップ型ＲＦＩＤデータ
暗証番号
電子証明書
その他アプリケーションソフト
モンデックス(リロード金額)
デビットカード情報
クレジットカード情報
ＶＰ氏名・住所
ＶＰＥメールアドレス
ＶＰの公開鍵KPと秘密鍵KS
ＲＰの認証鍵KN
ＶＰの年齢・職業等
ＶＰの各種嗜好情報
ＶＰの家族構成

【図９】

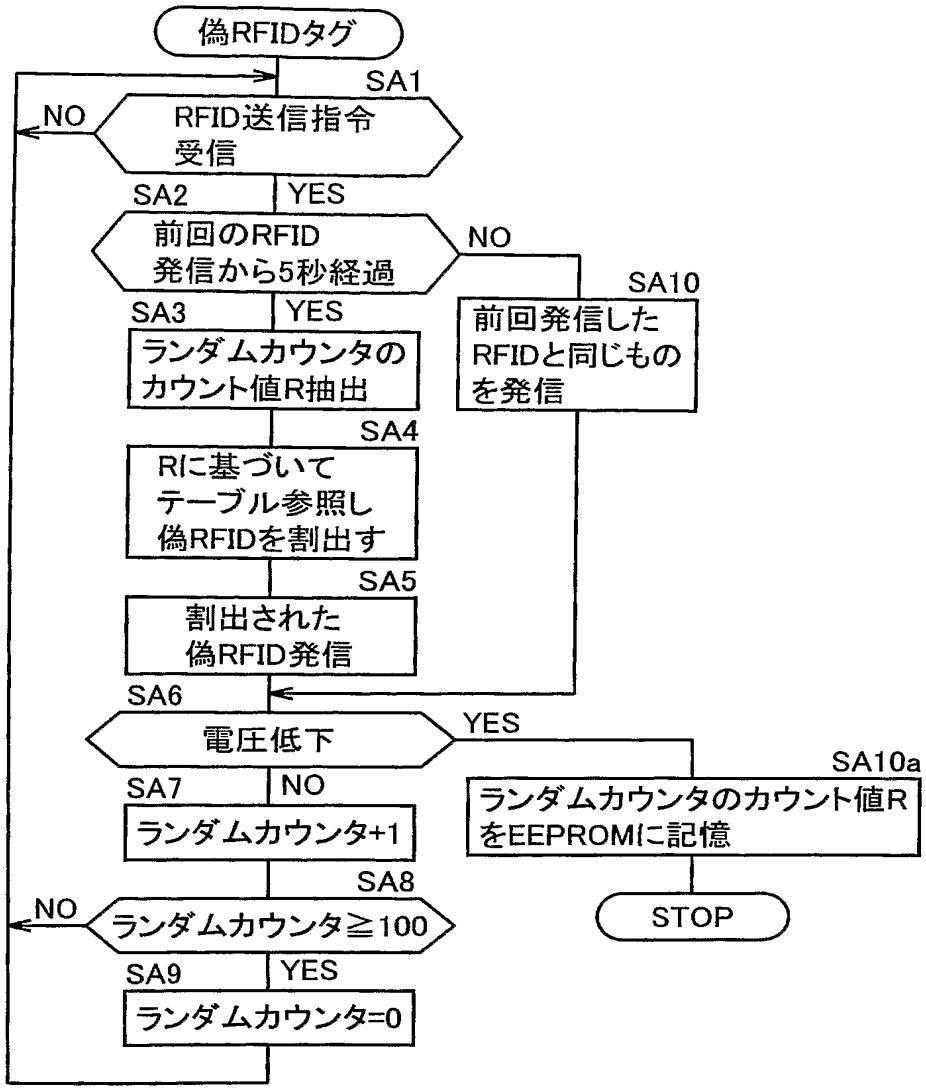


VP氏名	トラップ型RFID	業者名
B13P	abc,hij,amz,rak,・・・	ABC,HIJ,AMZ・・・
E(B13P)	mtt	MTT
E^2(B13P)	mec	MEC
E^3(B13P)	ktt	KTT
⋮	⋮	⋮

【図１０】


100
101
102
103
107a
ロジック
ROM
RAM
EEPROM
ループアンテナ
108
データバス
104
105
入出力制御部
変調・復調部
ループアンテナ
106
電源制御部
110
107b
1a
1

【図１１】


偽RFIDタグ
SA1
NO
RFID送信指令
受信
SA2
YES
前回のRFID
発信から5秒経過
NO
SA10
前回発信した
RFIDと同じもの
を発信
SA3
YES
ランダムカウンタの
カウント値R抽出
SA4
Rに基づいて
テーブル参照し
偽RFIDを割出す
SA5
割出された
偽RFID発信
SA6
電圧低下
YES
SA10a
ランダムカウンタのカウント値R
をEEPROMに記憶
SA7
NO
ランダムカウンタ+1
SA8
NO
ランダムカウンタ≧100
STOP
SA9
YES
ランダムカウンタ=0

【図１２】

(a)

R	0～39	40～54	55～69	70～84	85～99
RFID	820493176	730854709	813926081	791405731	835406912

(b)

R	0～39	40～54	55～69	70～84	85～99
RFID1	831709281	793102792	814358231	840526390	751052891
RFID2	779203980	809132041	849137655	789182509	850021934
RFID3	839093127	749084765	788015233	850139767	802049344
RFID4	740980346	808645210	779288401	750561234	766104988

(c)

R	0～39	40～54	55～69	70～84	85～99
RFID1	799804511	717950841	899893020	879010300	700913561
RFID2	779203980	709130241	749182655	889121509	750021214
RFID3	839093127	849048765	888062233	750161767	702049319
RFID4	740980346	708642510	879264401	850561202	856104923

【図１３】

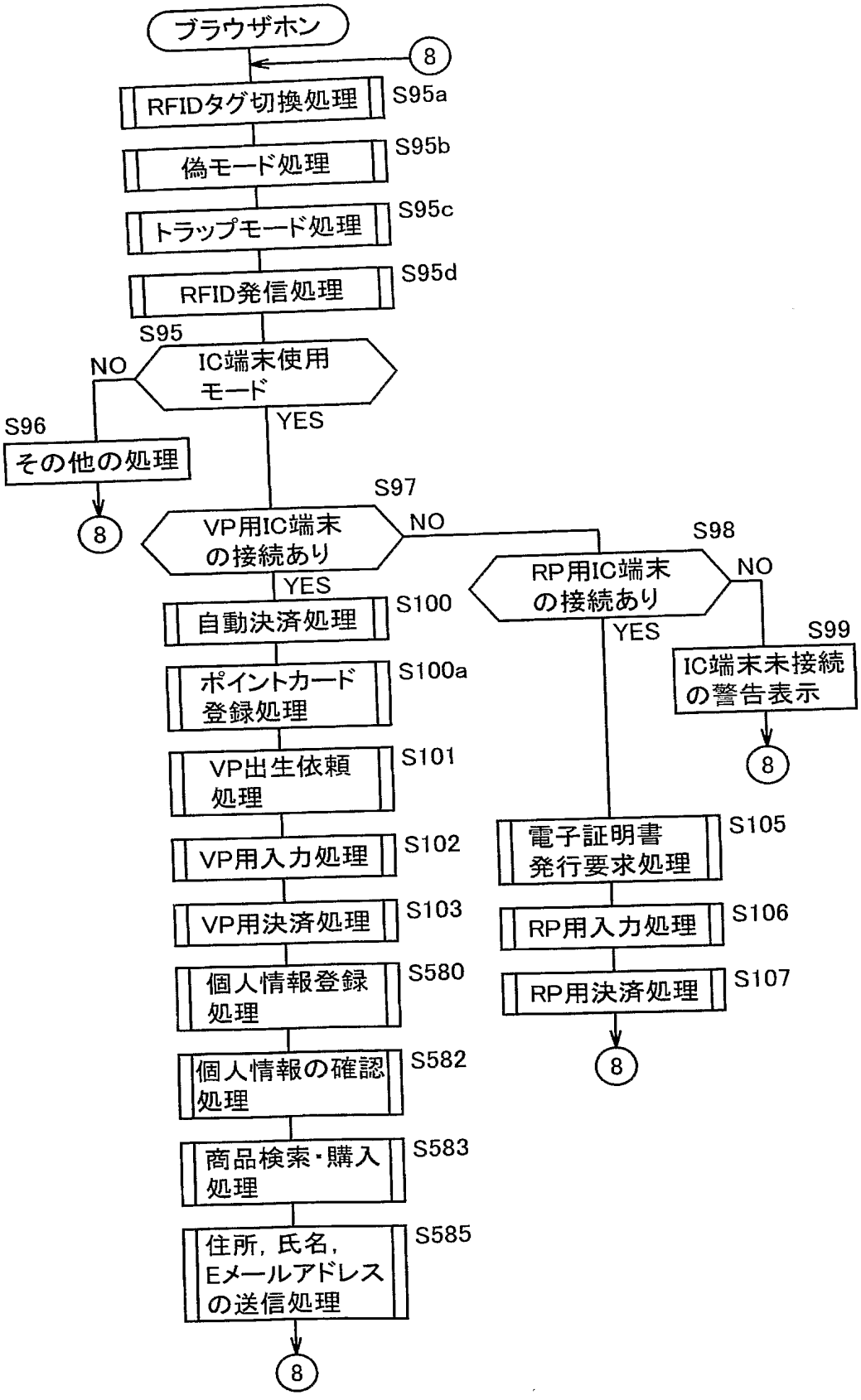
(a)

共通偽RFID	販売地域
820493176	千代田区
809207321	新宿区
831902845	渋谷区
∫	∫
798091320	右京区

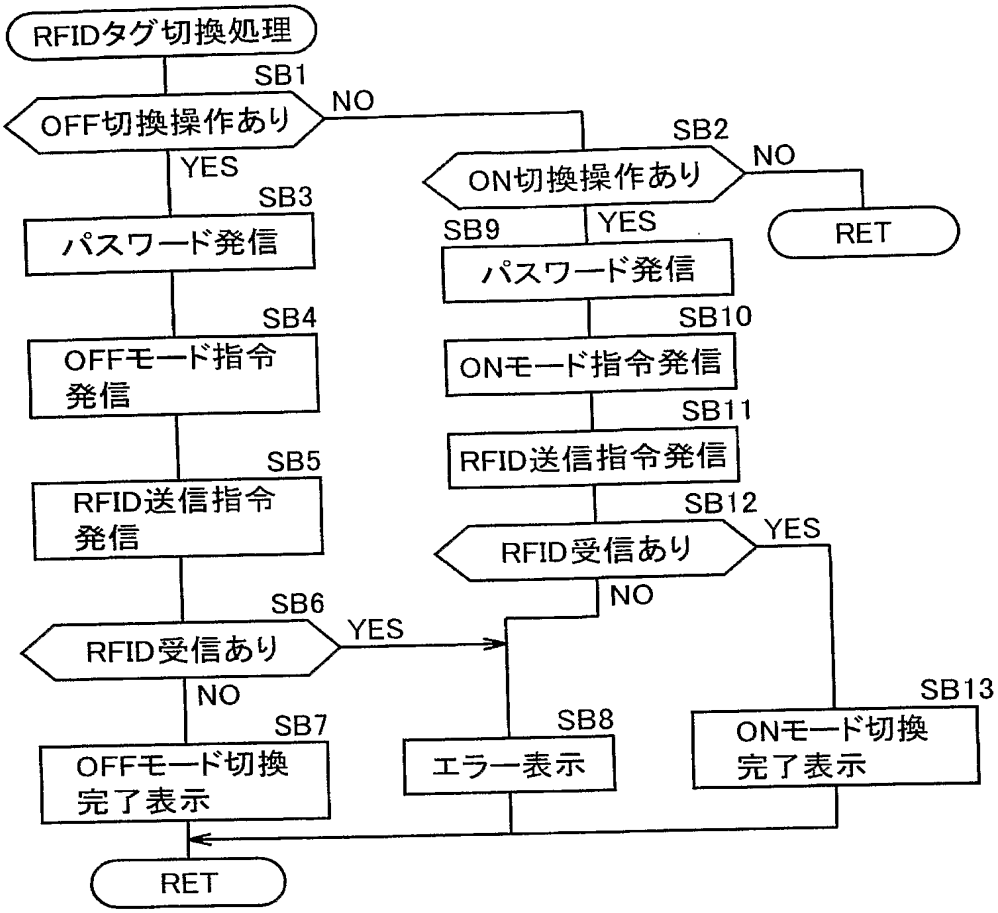
(b)

共通偽RFID	販売地域
779203980 839093127 740980346	千代田区
810391562 781529055 808892177	新宿区
∫	∫
788718955 845590329 822770945	右京区

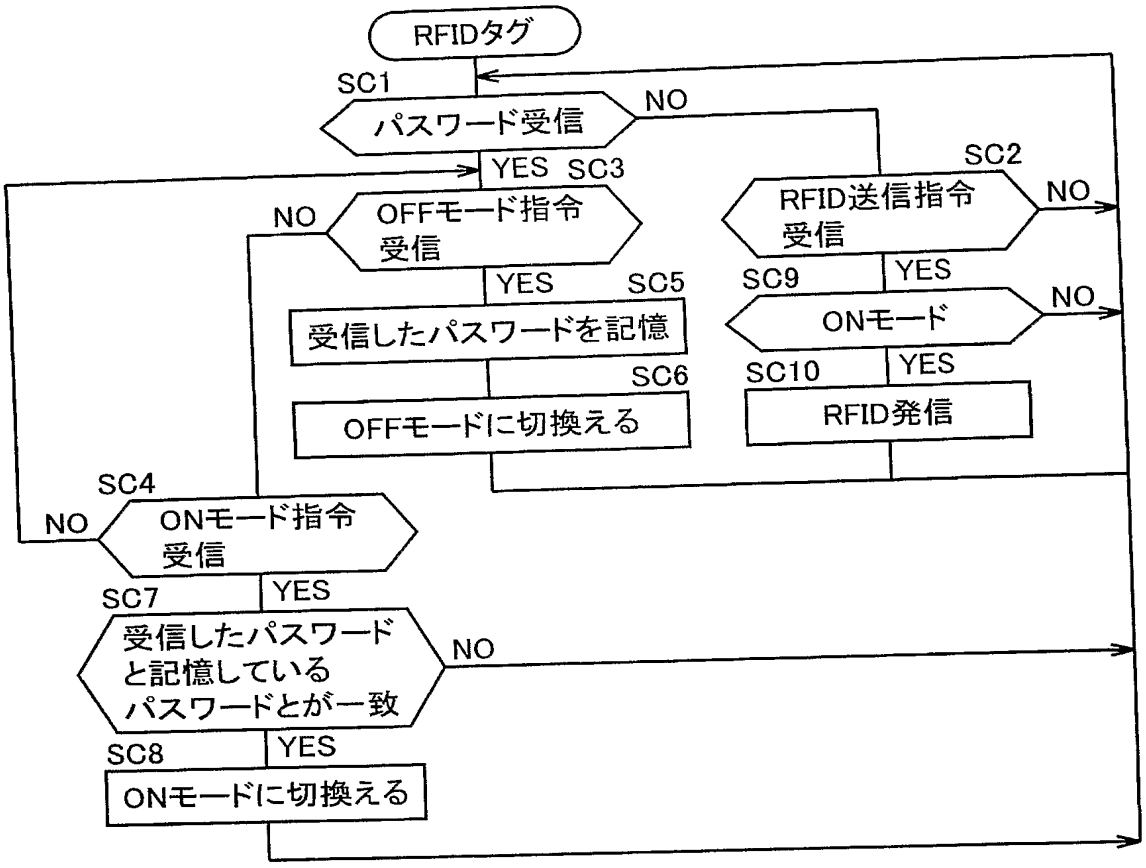
【図１４】


ブラウザホン
8
RFIDタグ切換処理
S95a
偽モード処理
S95b
トラップモード処理
S95c
RFID発信処理
S95d
S95
IC端末使用モード
NO
YES
S96
その他の処理
8
S97
VP用IC端末の接続あり
NO
YES
S98
RP用IC端末の接続あり
NO
YES
S99
IC端末未接続の警告表示
8
自動決済処理
S100
ポイントカード登録処理
S100a
VP出生依頼処理
S101
VP用入力処理
S102
VP用決済処理
S103
個人情報登録処理
S580
個人情報の確認処理
S582
商品検索・購入処理
S583
住所，氏名，Eメールアドレスの送信処理
S585
8
電子証明書発行要求処理
S105
RP用入力処理
S106
RP用決済処理
S107
8

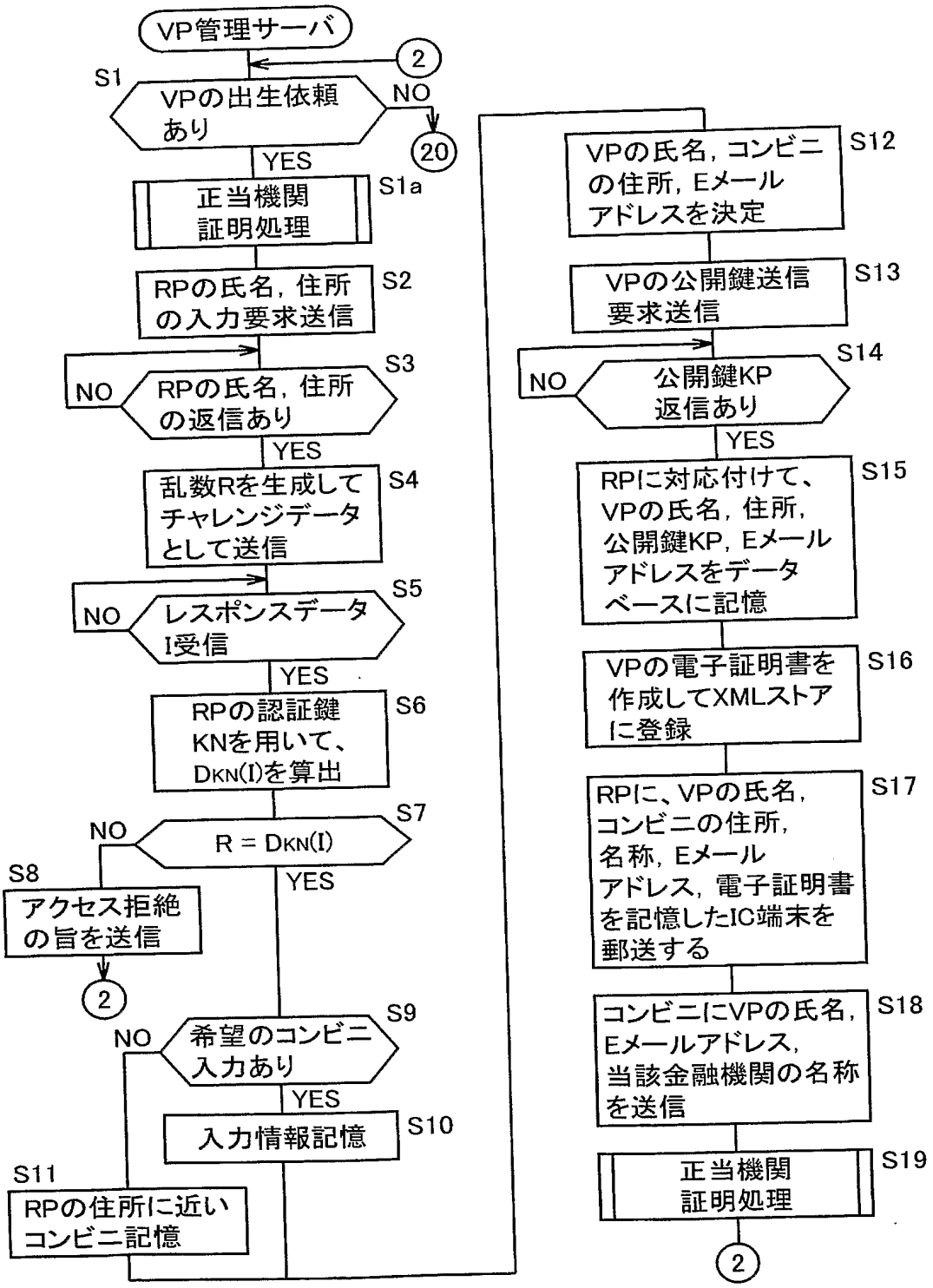
【図１５】


RFIDタグ切換処理
SB1
OFF切換操作あり
NO
YES
SB2
ON切換操作あり
NO
RET
SB3
パスワード発信
SB9
YES
パスワード発信
SB4
OFFモード指令発信
SB10
ONモード指令発信
SB11
RFID送信指令発信
SB5
RFID送信指令発信
SB12
RFID受信あり
YES
NO
SB6
RFID受信あり
YES
NO
SB13
ONモード切換完了表示
SB7
OFFモード切換完了表示
SB8
エラー表示
RET

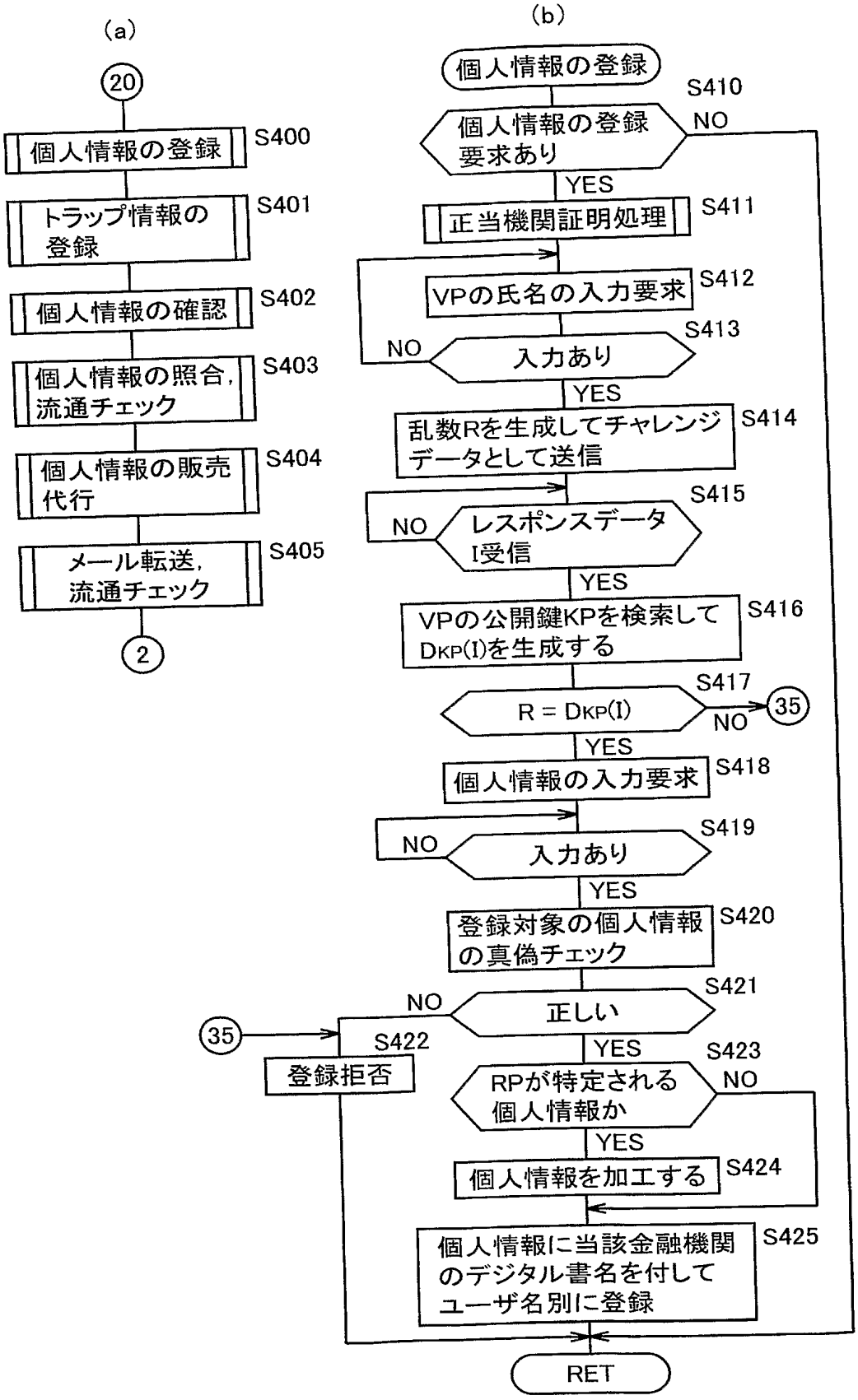
【図１６】


RFIDタグ
SC1
パスワード受信
NO
YES
SC3
OFFモード指令受信
NO
YES
SC5
受信したパスワードを記憶
SC6
OFFモードに切換える
SC4
ONモード指令受信
NO
SC7
YES
受信したパスワードと記憶しているパスワードとが一致
NO
SC8
YES
ONモードに切換える
SC2
RFID送信指令受信
NO
SC9
YES
ONモード
NO
SC10
YES
RFID発信

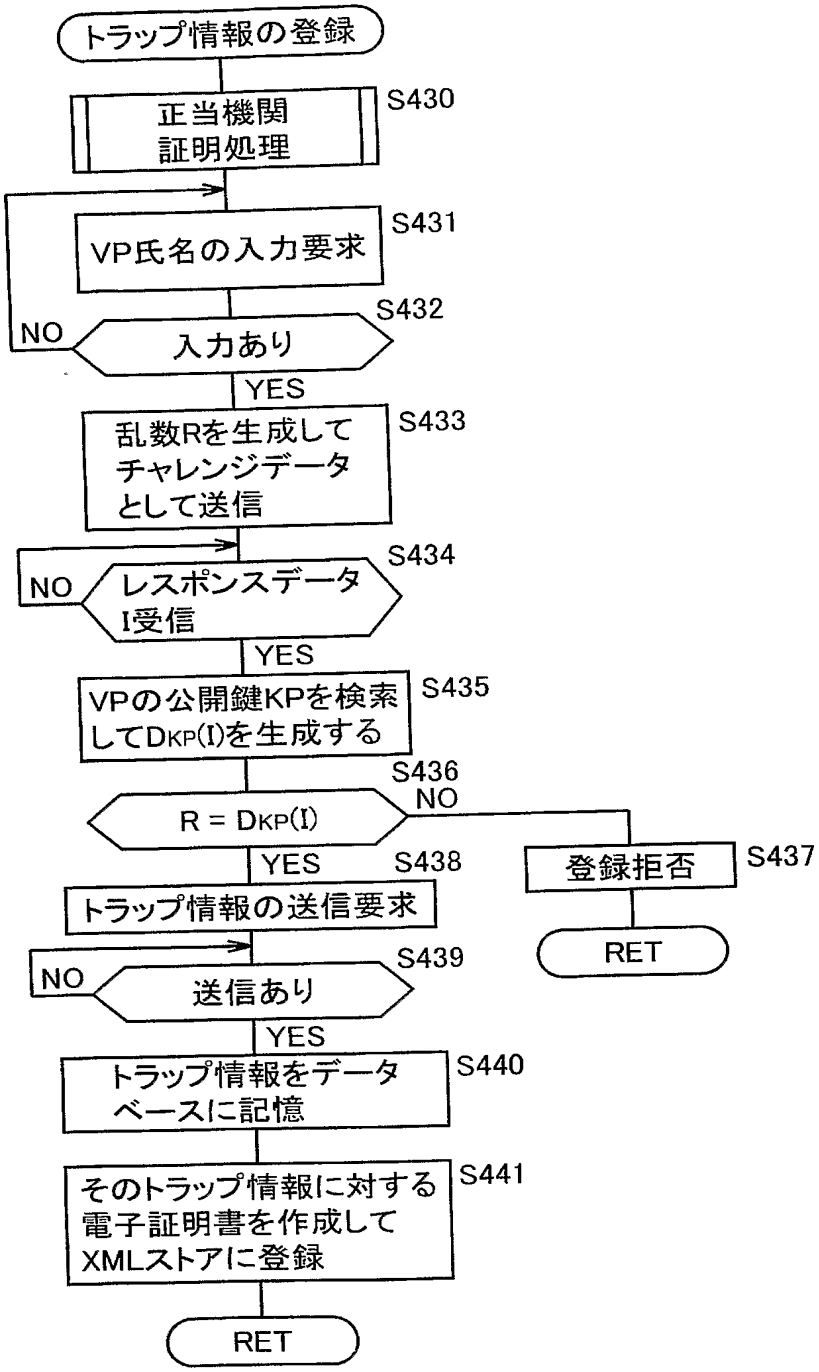
【図１７】


VP管理サーバ
2
S1
VPの出生依頼あり
NO
20
YES
正当機関証明処理
S1a
RPの氏名，住所の入力要求送信
S2
NO
RPの氏名，住所の返信あり
S3
YES
乱数Rを生成してチャレンジデータとして送信
S4
NO
レスポンスデータI受信
S5
YES
RPの認証鍵KNを用いて、DKN(I)を算出
S6
NO
R = DKN(I)
S7
YES
S8
アクセス拒絶の旨を送信
2
NO
希望のコンビニ入力あり
S9
YES
入力情報記憶
S10
S11
RPの住所に近いコンビニ記憶
VPの氏名，コンビニの住所，Eメールアドレスを決定
S12
VPの公開鍵送信要求送信
S13
NO
公開鍵KP返信あり
S14
YES
RPに対応付けて、VPの氏名，住所，公開鍵KP，Eメールアドレスをデータベースに記憶
S15
VPの電子証明書を作成してXMLストアに登録
S16
RPに、VPの氏名，コンビニの住所，名称，Eメールアドレス，電子証明書を記憶したIC端末を郵送する
S17
コンビニにVPの氏名，Eメールアドレス，当該金融機関の名称を送信
S18
正当機関証明処理
S19
2

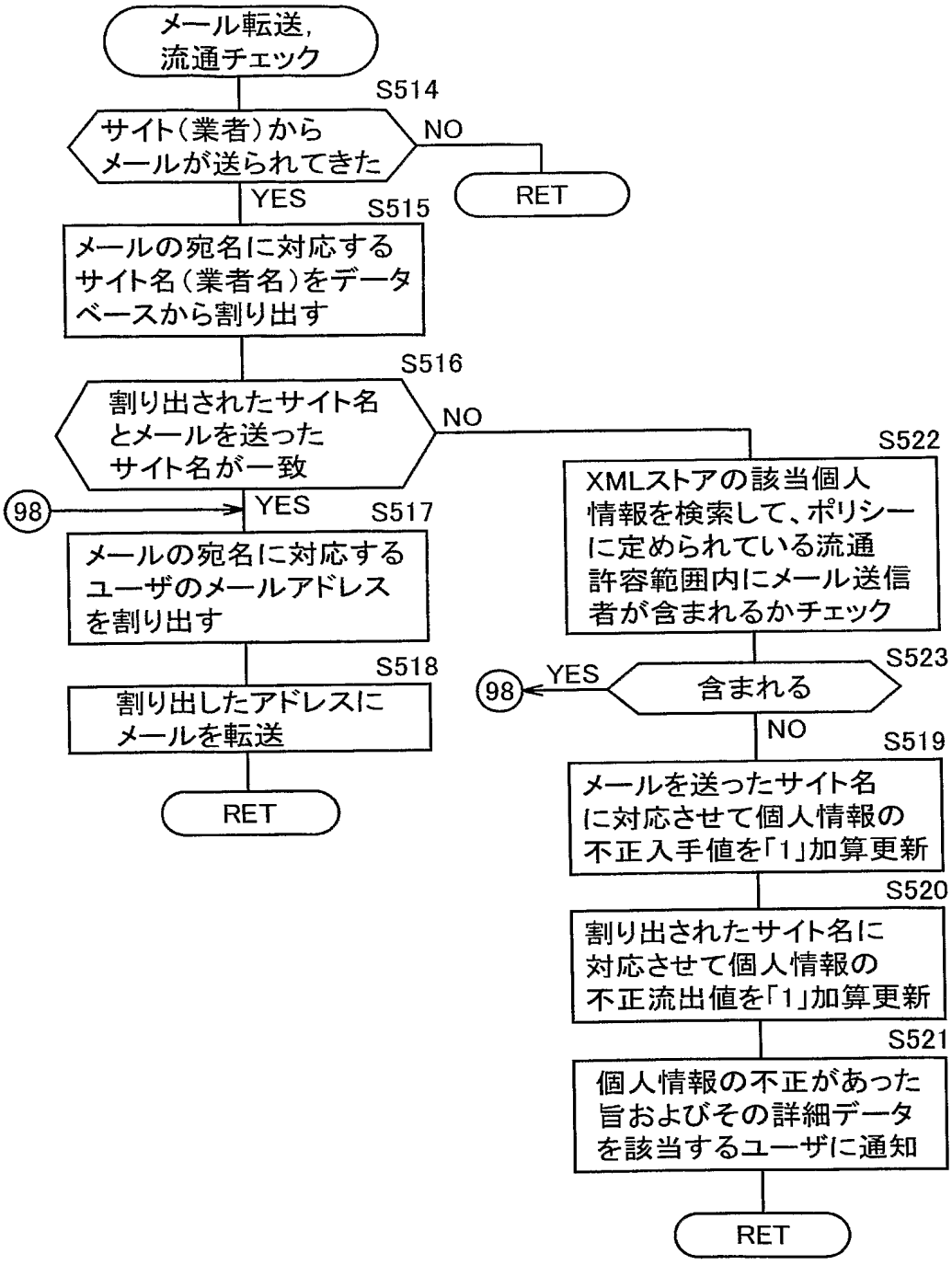
【図１８】


(a)
20
個人情報の登録
S400
トラップ情報の登録
S401
個人情報の確認
S402
個人情報の照合，流通チェック
S403
個人情報の販売代行
S404
メール転送，流通チェック
S405
2
(b)
個人情報の登録
S410
個人情報の登録要求あり
NO
YES
正当機関証明処理
S411
VPの氏名の入力要求
S412
S413
NO
入力あり
YES
乱数Rを生成してチャレンジデータとして送信
S414
S415
NO
レスポンスデータI受信
YES
VPの公開鍵KPを検索してDKP(I)を生成する
S416
S417
R = DKP(I)
NO
35
YES
個人情報の入力要求
S418
NO
S419
入力あり
YES
登録対象の個人情報の真偽チェック
S420
NO
S421
正しい
35
S422
登録拒否
YES
S423
RPが特定される個人情報か
NO
YES
個人情報を加工する
S424
個人情報に当該金融機関のデジタル書名を付してユーザ名別に登録
S425
RET

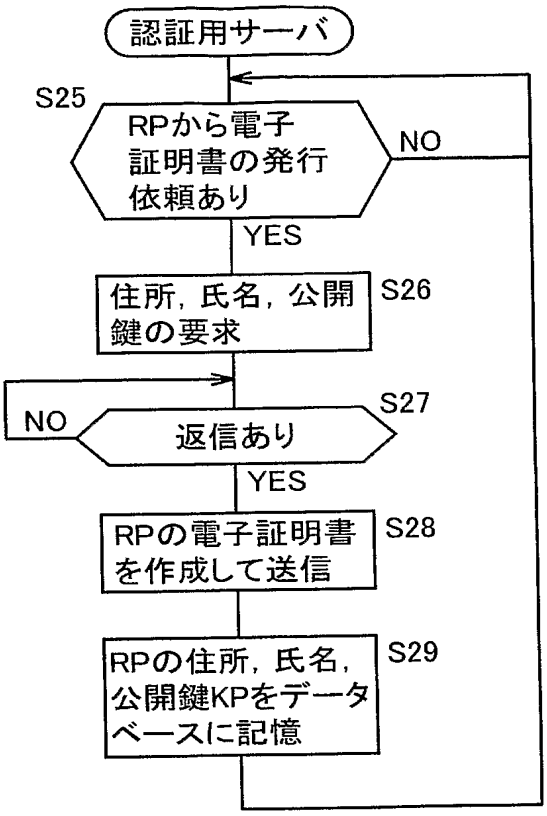
【図１９】


トラップ情報の登録
正当機関
証明処理
S430
VP氏名の入力要求
S431
NO
入力あり
S432
YES
乱数Rを生成して
チャレンジデータ
として送信
S433
NO
レスポンスデータ
I受信
S434
YES
VPの公開鍵KPを検索
してDKP(I)を生成する
S435
S436
R = DKP(I)
NO
登録拒否
S437
RET
YES
S438
トラップ情報の送信要求
NO
送信あり
S439
YES
トラップ情報をデータ
ベースに記憶
S440
そのトラップ情報に対する
電子証明書を作成して
XMLストアに登録
S441
RET

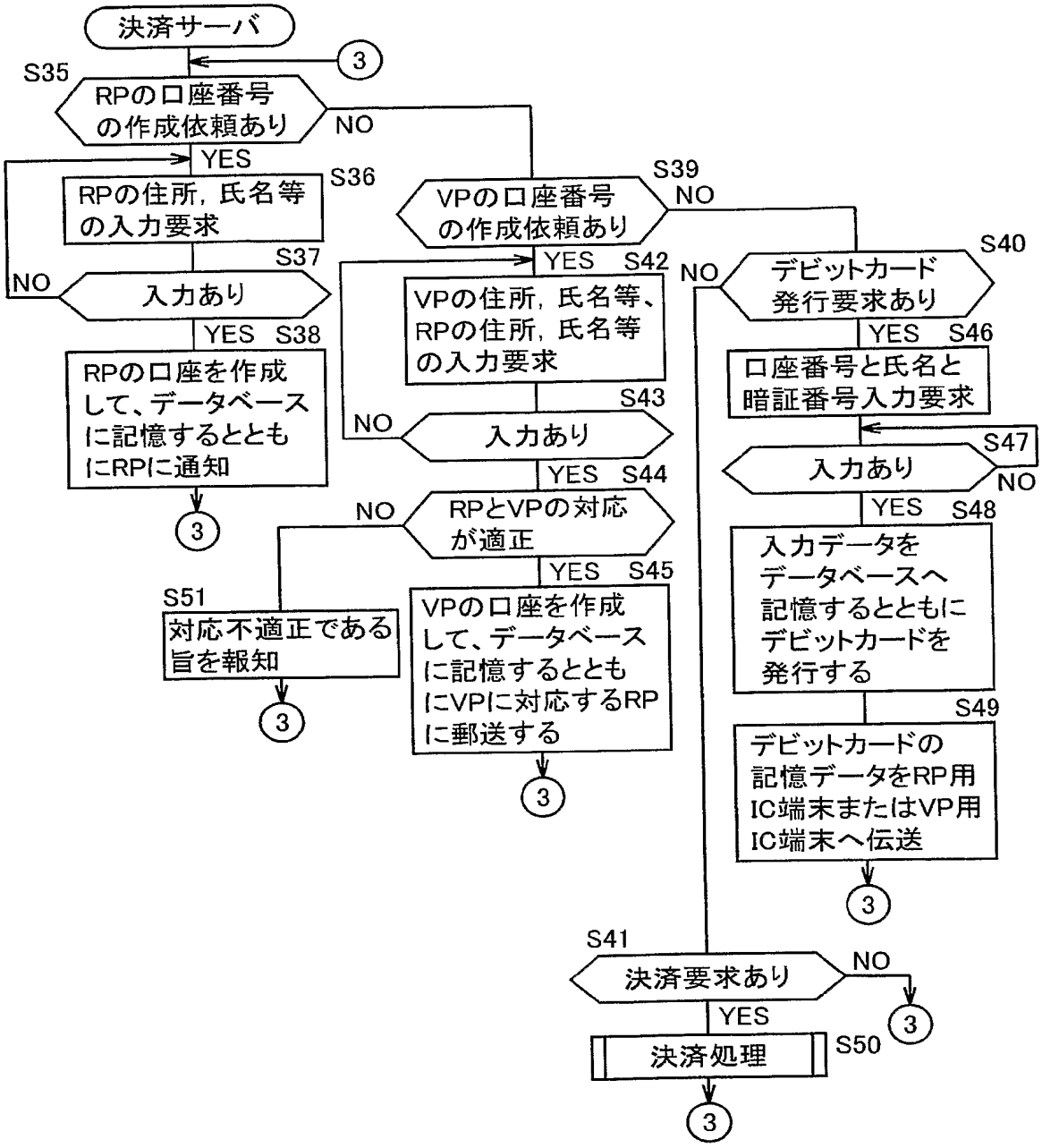
【図２０】


メール転送，
流通チェック
S514
サイト（業者）から
メールが送られてきた
NO
RET
YES
S515
メールの宛名に対応する
サイト名（業者名）をデータ
ベースから割り出す
S516
割り出されたサイト名
とメールを送った
サイト名が一致
NO
S522
XMLストアの該当個人
情報を検索して、ポリシー
に定められている流通
許容範囲内にメール送信
者が含まれるかチェック
98
YES
S517
メールの宛名に対応する
ユーザのメールアドレス
を割り出す
S523
98
YES
含まれる
NO
S518
割り出したアドレスに
メールを転送
S519
メールを送ったサイト名
に対応させて個人情報の
不正入手値を「1」加算更新
RET
S520
割り出されたサイト名に
対応させて個人情報の
不正流出値を「1」加算更新
S521
個人情報の不正があった
旨およびその詳細データ
を該当するユーザに通知
RET

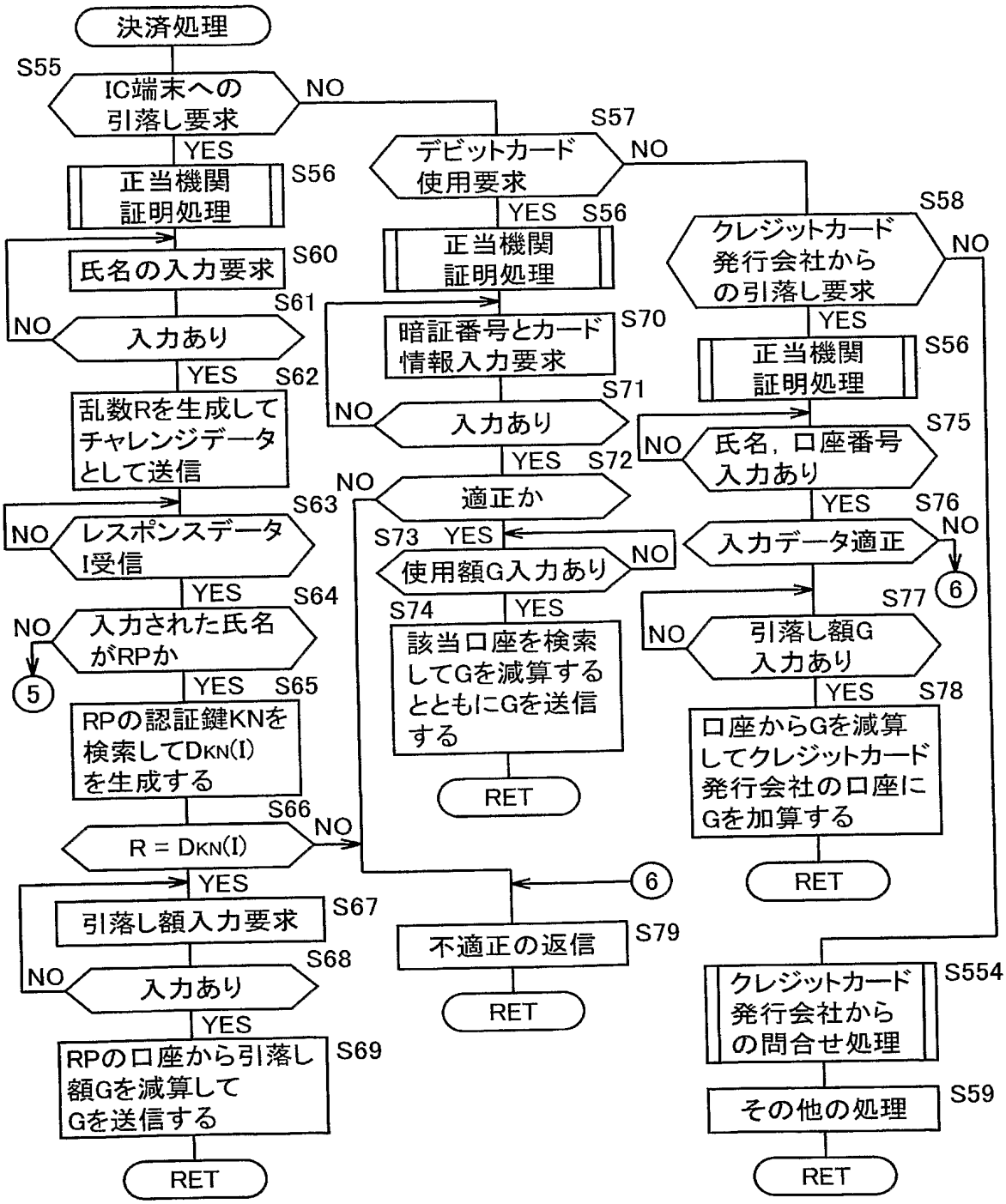
【図２１】


認証用サーバ
S25
RPから電子証明書の発行依頼あり
NO
YES
住所，氏名，公開鍵の要求
S26
NO
返信あり
S27
YES
RPの電子証明書を作成して送信
S28
RPの住所，氏名，公開鍵KPをデータベースに記憶
S29

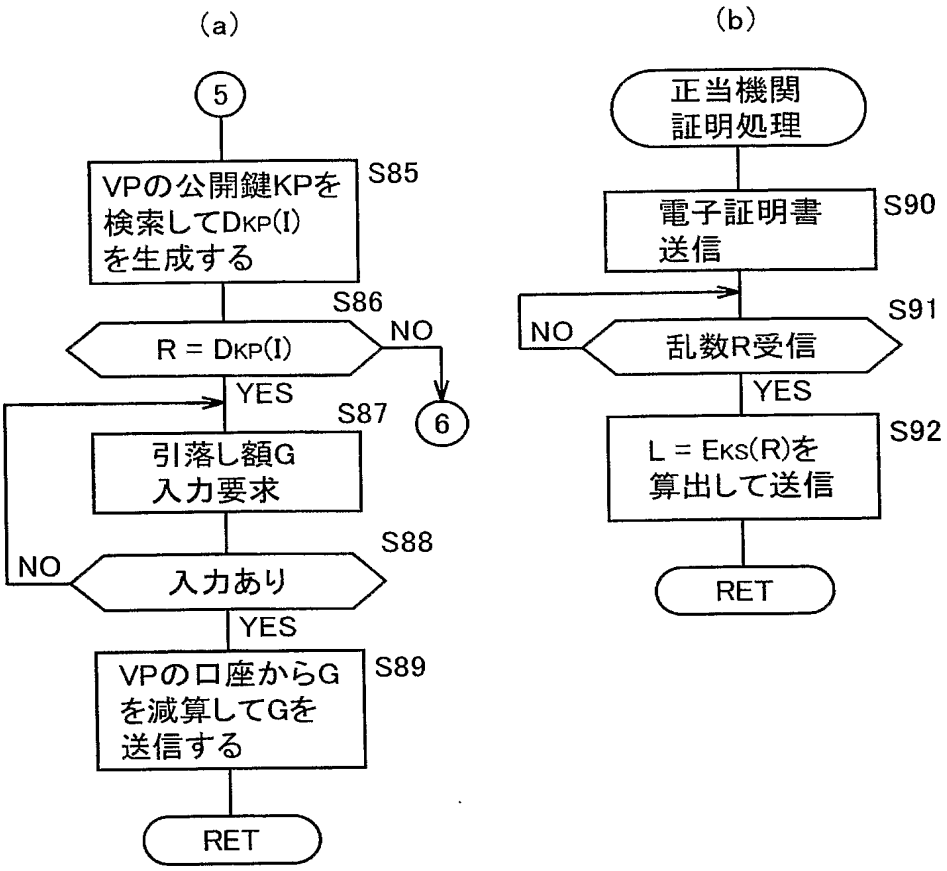
【図２２】


決済サーバ
3
S35
RPの口座番号の作成依頼あり
NO
YES
S36
RPの住所，氏名等の入力要求
S37
NO
入力あり
YES S38
RPの口座を作成して、データベースに記憶するとともにRPに通知
3
S39
VPの口座番号の作成依頼あり
NO
YES S42
VPの住所，氏名等、RPの住所，氏名等の入力要求
S43
NO
入力あり
YES S44
NO
RPとVPの対応が適正
YES S45
S51
対応不適正である旨を報知
3
VPの口座を作成して、データベースに記憶するとともにVPに対応するRPに郵送する
3
S40
NO
デビットカード発行要求あり
YES S46
口座番号と氏名と暗証番号入力要求
S47
入力あり
NO
YES S48
入力データをデータベースへ記憶するとともにデビットカードを発行する
S49
デビットカードの記憶データをRP用IC端末またはVP用IC端末へ伝送
3
S41
決済要求あり
NO
3
YES
決済処理
S50
3

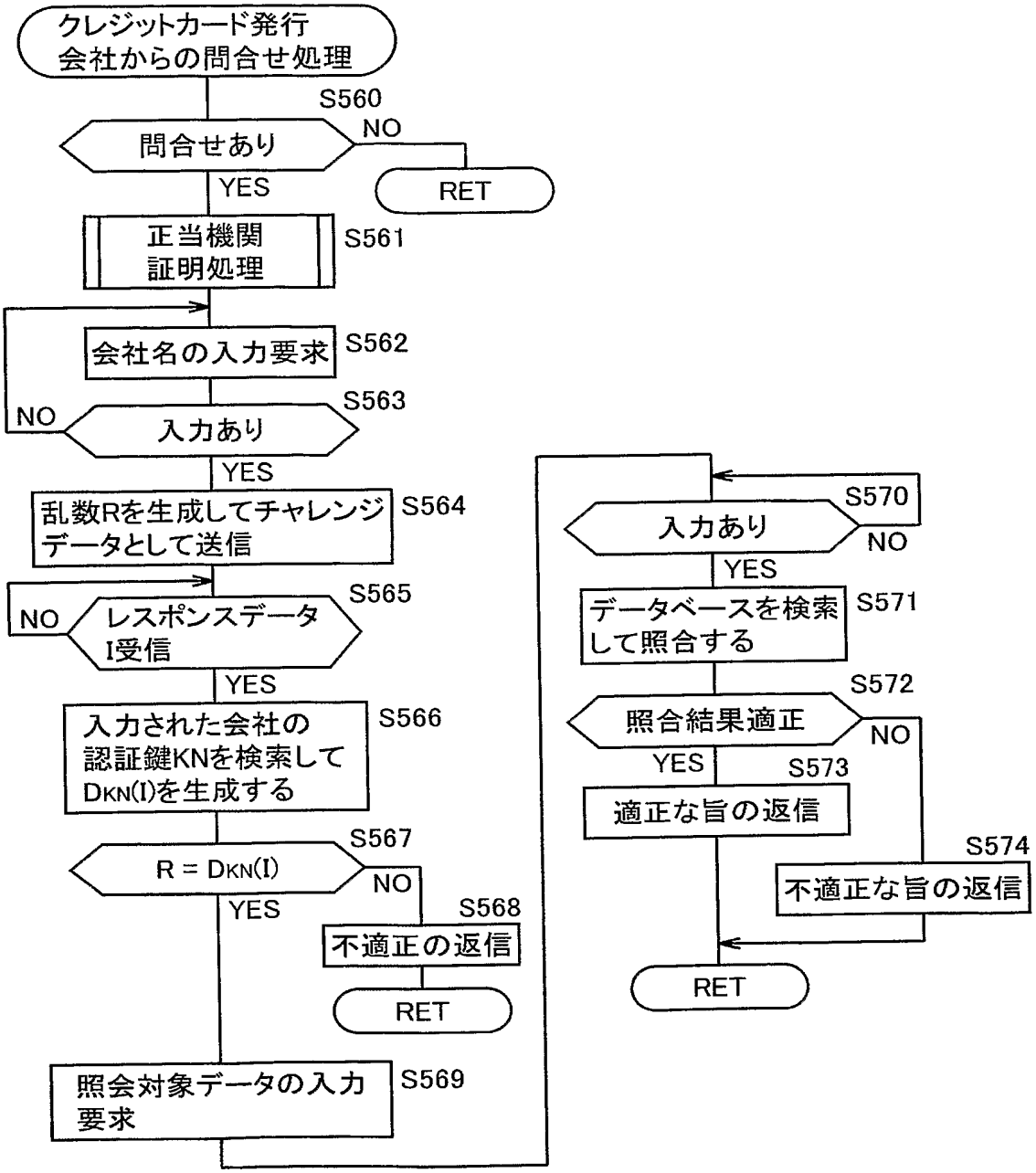
【図２３】


決済処理
S55
IC端末への引落し要求
NO
YES
S57
デビットカード使用要求
NO
YES
S56
正当機関証明処理
S58
クレジットカード発行会社からの引落し要求
NO
YES
S56
正当機関証明処理
S60
氏名の入力要求
S61
NO
入力あり
YES
S62
乱数Rを生成してチャレンジデータとして送信
S63
NO
レスポンスデータI受信
YES
S64
NO
入力された氏名がRPか
YES
S65
RPの認証鍵KNを検索してDKN(I)を生成する
S66
R = DKN(I)
NO
YES
S67
引落し額入力要求
S68
NO
入力あり
YES
S69
RPの口座から引落し額Gを減算してGを送信する
RET
5
S70
暗証番号とカード情報入力要求
S71
NO
入力あり
YES
S72
NO
適正か
S73
YES
使用額G入力あり
NO
S74
YES
該当口座を検索してGを減算するとともにGを送信する
RET
6
不適正の返信
S79
RET
S75
NO
氏名，口座番号入力あり
YES
S76
入力データ適正
NO
6
S77
NO
引落し額G入力あり
YES
S78
口座からGを減算してクレジットカード発行会社の口座にGを加算する
RET
S554
クレジットカード発行会社からの問合せ処理
S59
その他の処理
RET

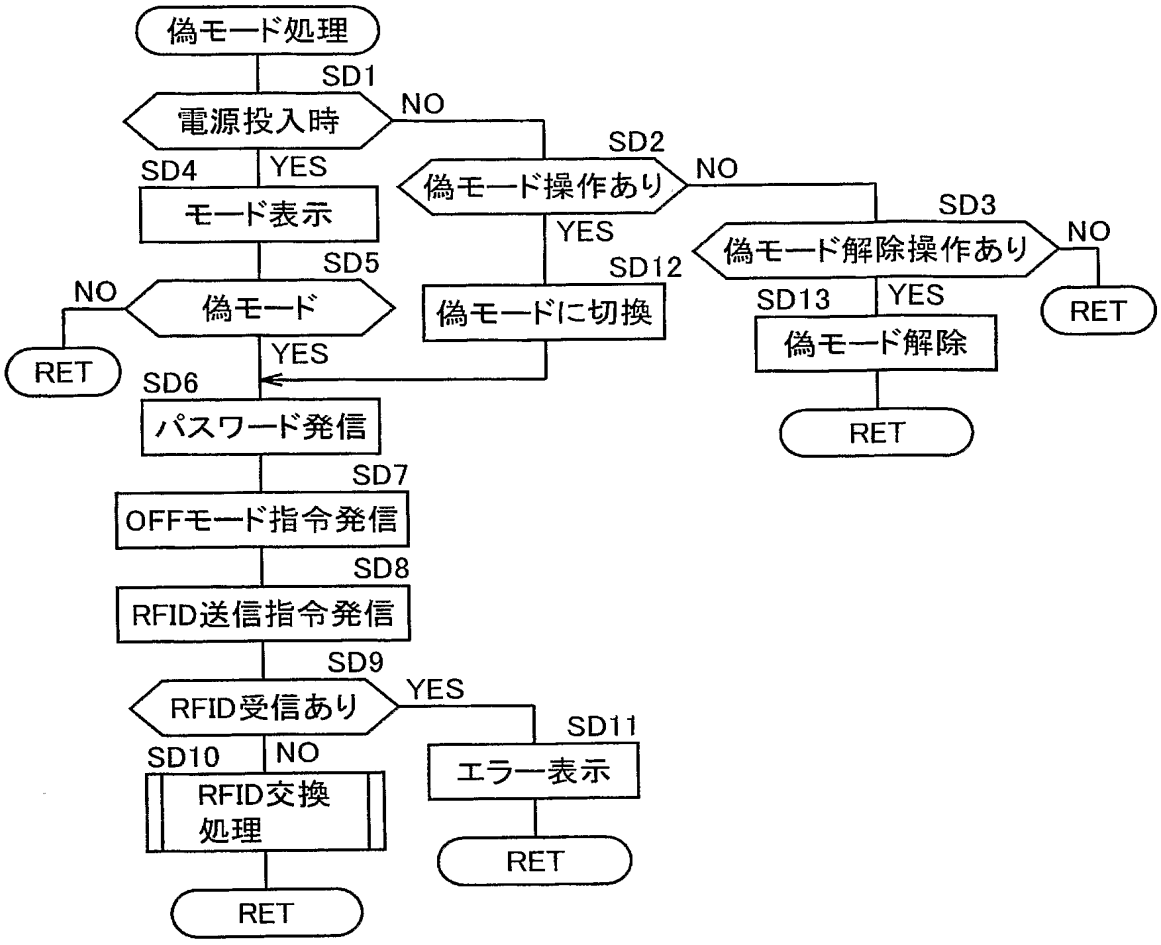
【図２４】


(a)
5
VPの公開鍵KPを検索してDKP(I)を生成する
S85
S86
R = DKP(I)
NO
YES
6
S87
引落し額G入力要求
S88
NO
入力あり
YES
VPの口座からGを減算してGを送信する
S89
RET
(b)
正当機関証明処理
電子証明書送信
S90
S91
NO
乱数R受信
YES
L = EKS(R)を算出して送信
S92
RET

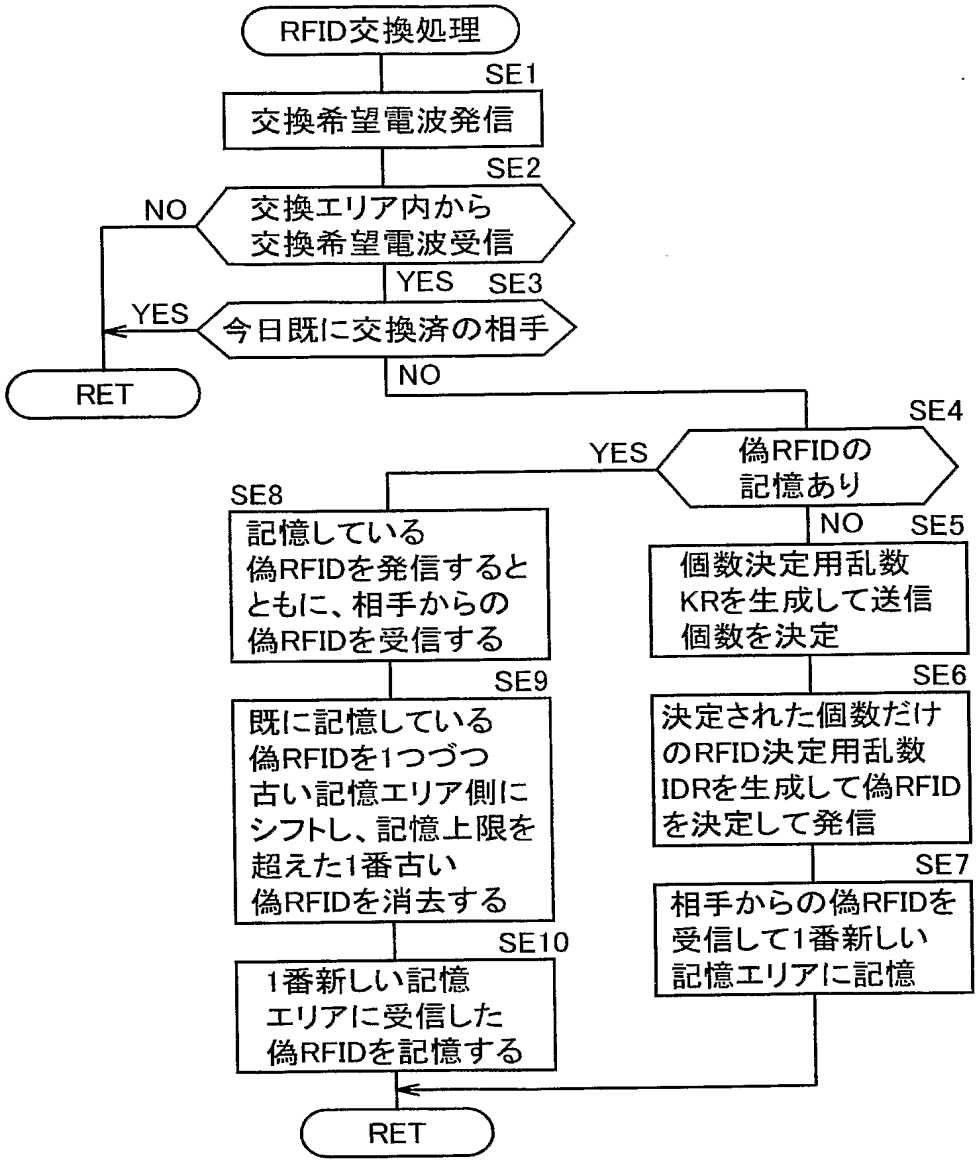
【図２５】


クレジットカード発行
会社からの問合せ処理
S560
問合せあり
NO
RET
YES
正当機関
証明処理
S561
会社名の入力要求
S562
NO
入力あり
S563
YES
乱数Rを生成してチャレンジ
データとして送信
S564
NO
レスポンスデータ
I受信
S565
YES
入力された会社の
認証鍵KNを検索して
DKN(I)を生成する
S566
R = DKN(I)
S567
NO
YES
不適正の返信
S568
RET
照会対象データの入力
要求
S569
入力あり
S570
NO
YES
データベースを検索
して照合する
S571
照合結果適正
S572
NO
YES
S573
適正な旨の返信
不適正な旨の返信
S574
RET

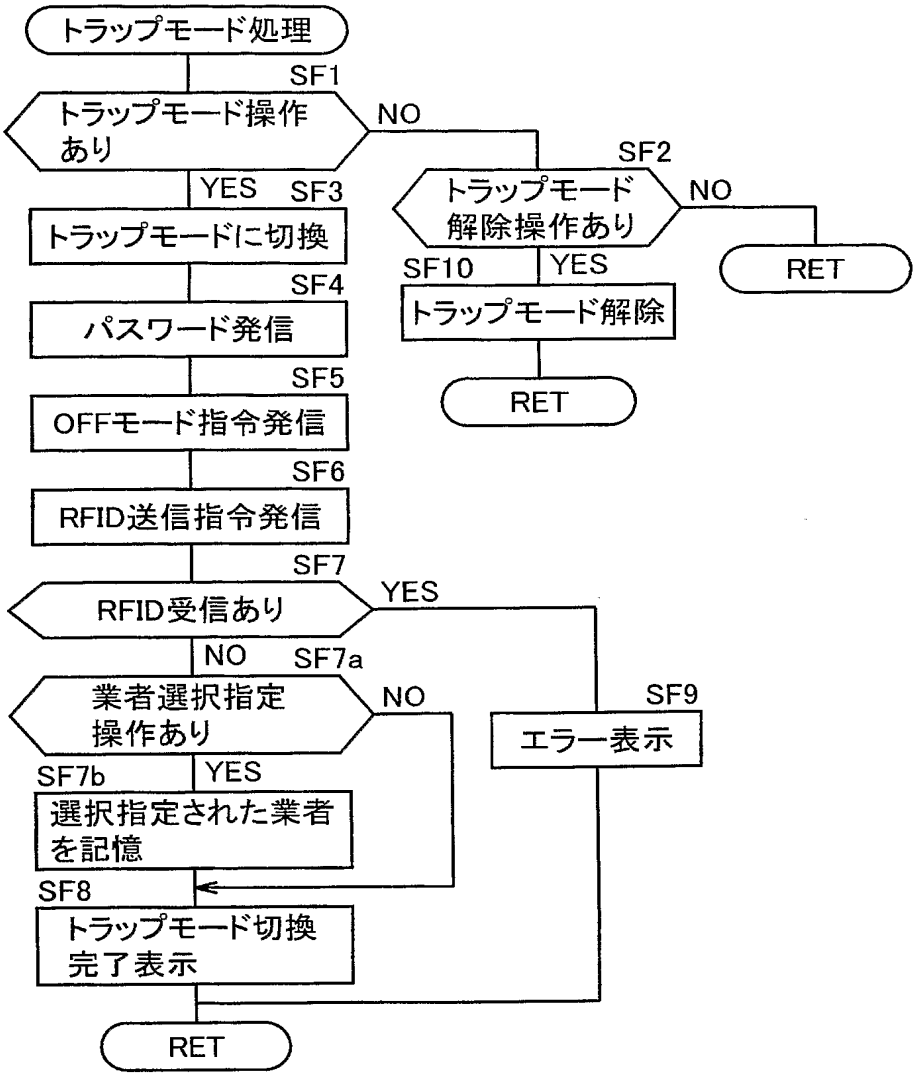
【図２６】


偽モード処理
SD1
電源投入時
NO
SD2
偽モード操作あり
NO
SD3
偽モード解除操作あり
NO
RET
SD4
YES
モード表示
YES
SD12
偽モードに切換
SD13
YES
偽モード解除
RET
SD5
偽モード
NO
RET
YES
SD6
パスワード発信
SD7
OFFモード指令発信
SD8
RFID送信指令発信
SD9
RFID受信あり
YES
SD11
エラー表示
RET
SD10
NO
RFID交換処理
RET

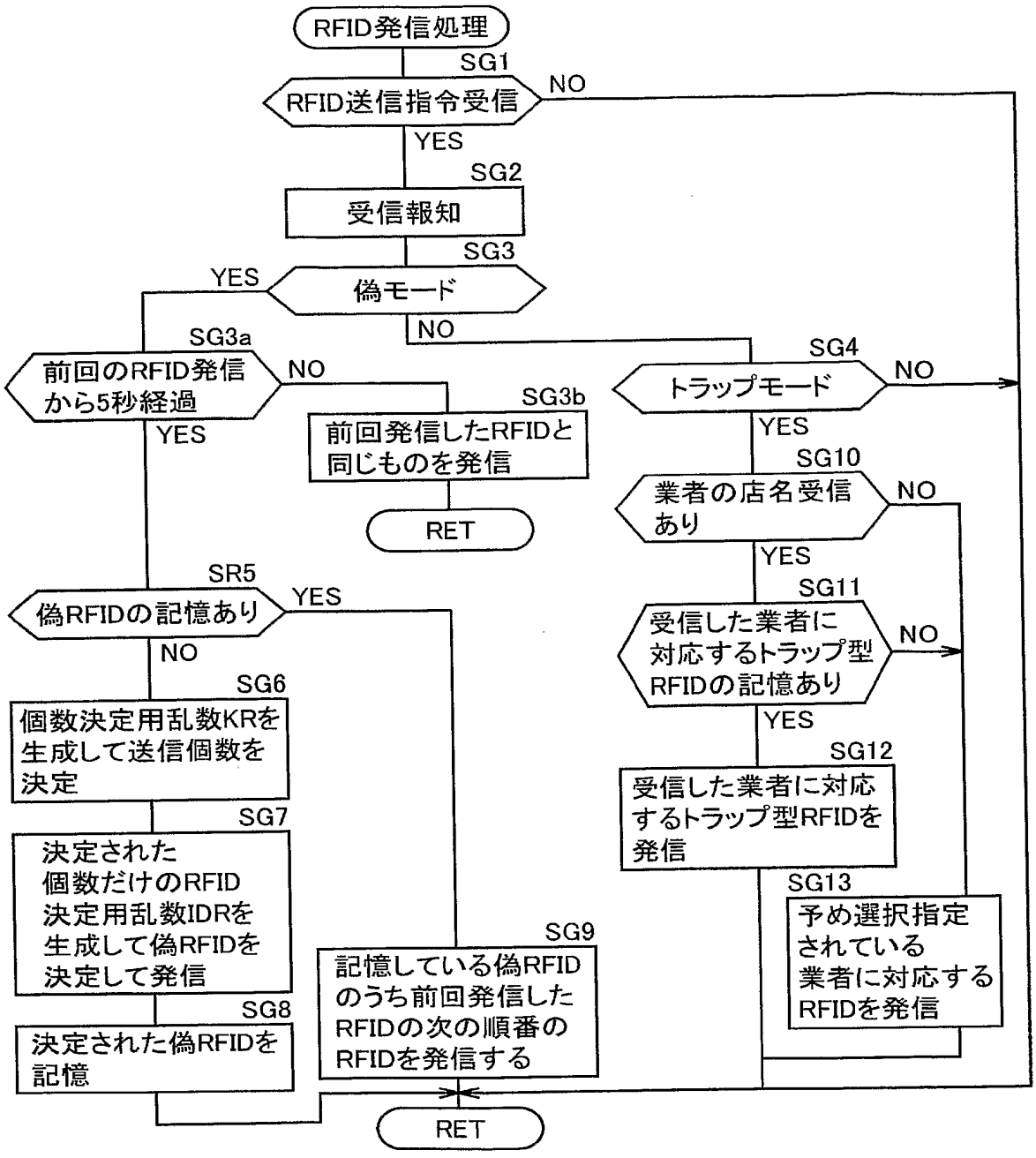
【図２７】


RFID交換処理
SE1
交換希望電波発信
SE2
交換エリア内から
交換希望電波受信
NO
YES
SE3
今日既に交換済の相手
YES
NO
RET
SE4
偽RFIDの
記憶あり
YES
NO
SE5
個数決定用乱数
KRを生成して送信
個数を決定
SE6
決定された個数だけ
のRFID決定用乱数
IDRを生成して偽RFID
を決定して発信
SE7
相手からの偽RFIDを
受信して1番新しい
記憶エリアに記憶
SE8
記憶している
偽RFIDを発信すると
ともに、相手からの
偽RFIDを受信する
SE9
既に記憶している
偽RFIDを1つづつ
古い記憶エリア側に
シフトし、記憶上限を
超えた1番古い
偽RFIDを消去する
SE10
1番新しい記憶
エリアに受信した
偽RFIDを記憶する
RET

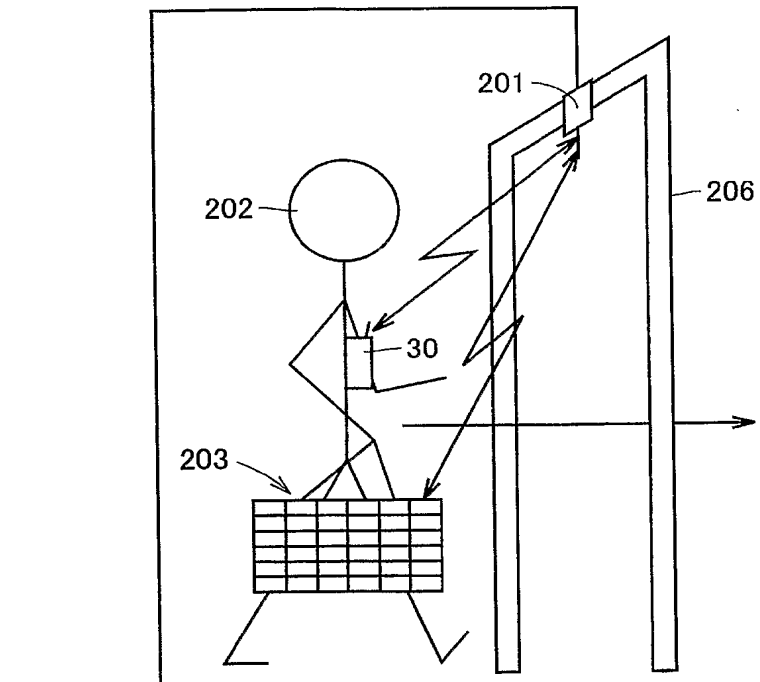
【図２８】

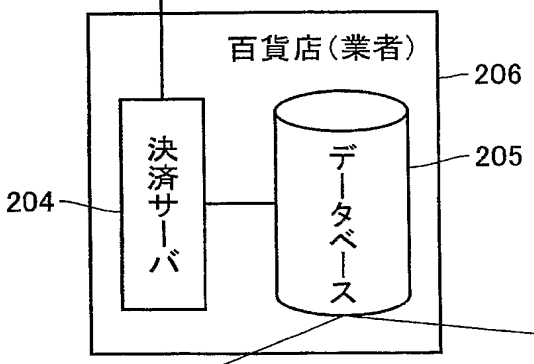

トラップモード処理
SF1
トラップモード操作あり
NO
YES
SF3
トラップモードに切換
SF4
パスワード発信
SF5
OFFモード指令発信
SF6
RFID送信指令発信
SF7
RFID受信あり
YES
NO
SF7a
業者選択指定操作あり
NO
SF7b
YES
選択指定された業者を記憶
SF8
トラップモード切換完了表示
RET
SF2
トラップモード解除操作あり
NO
RET
SF10
YES
トラップモード解除
RET
SF9
エラー表示

【図２９】


RFID発信処理
SG1
RFID送信指令受信
NO
YES
SG2
受信報知
SG3
偽モード
YES
NO
SG3a
前回のRFID発信から5秒経過
NO
YES
SG3b
前回発信したRFIDと同じものを発信
RET
SG4
トラップモード
NO
YES
SG10
業者の店名受信あり
NO
YES
SG11
受信した業者に対応するトラップ型RFIDの記憶あり
NO
YES
SG12
受信した業者に対応するトラップ型RFIDを発信
SG13
予め選択指定されている業者に対応するRFIDを発信
SR5
偽RFIDの記憶あり
YES
NO
SG6
個数決定用乱数KRを生成して送信個数を決定
SG7
決定された個数だけのRFID決定用乱数IDRを生成して偽RFIDを決定して発信
SG8
決定された偽RFIDを記憶
SG9
記憶している偽RFIDのうち前回発信したRFIDの次の順番のRFIDを発信する
RET

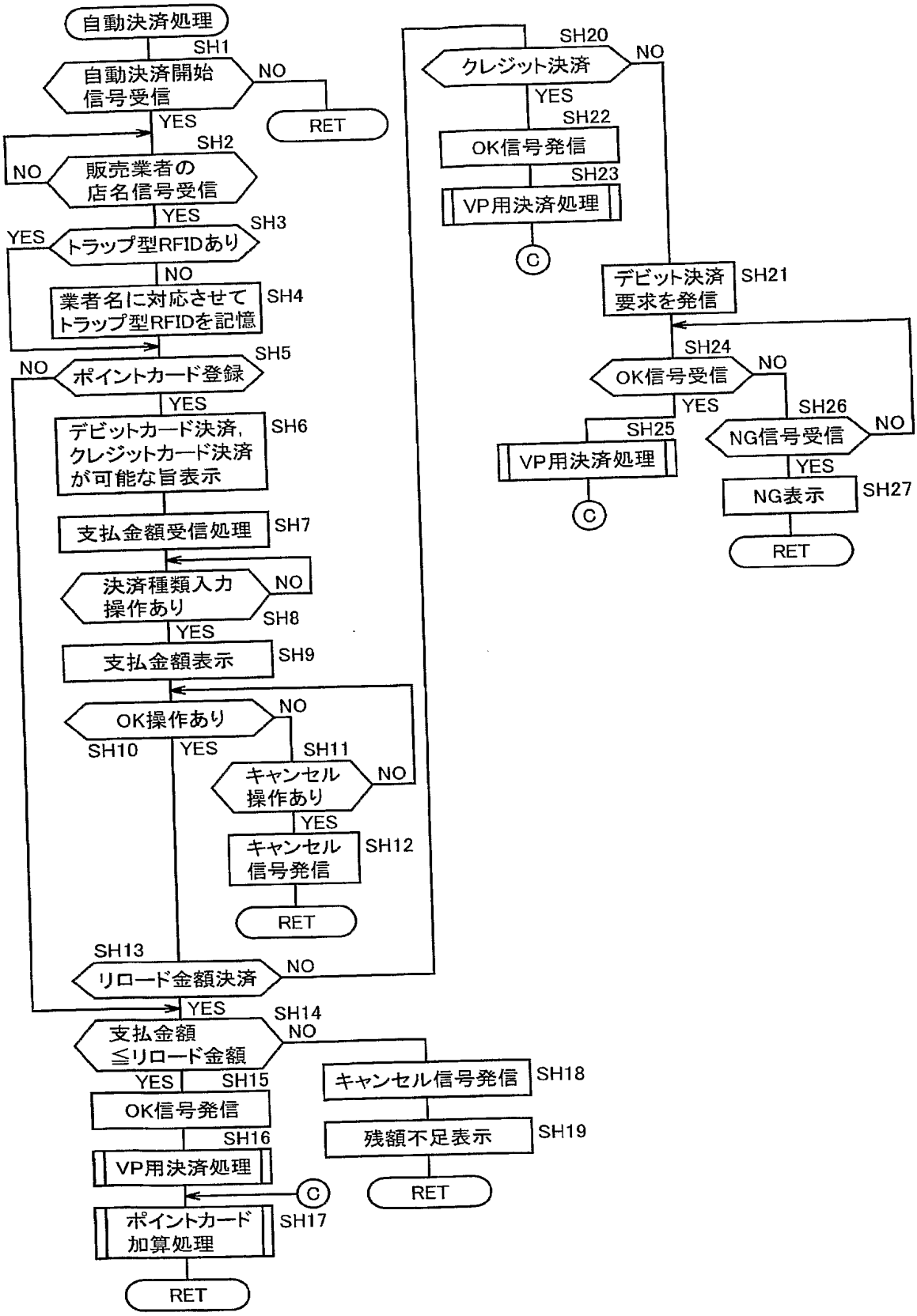
【図３０】



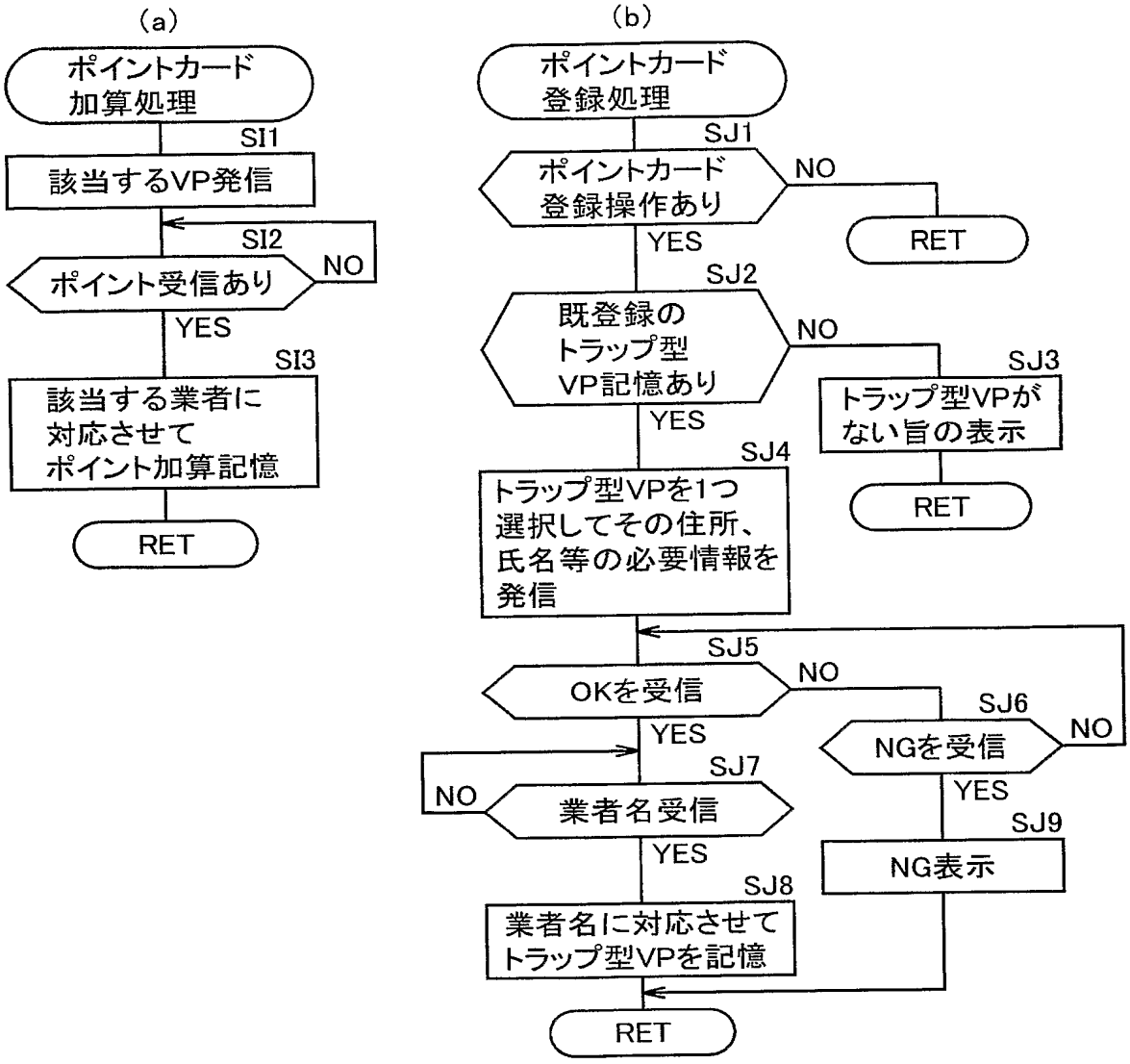


顧客名	ポイント数	住所	Eメールアドレス	バーチャル口座番号
E(B13P)	19018	□×○	△△△△△	E(2503)
E(NPXA)	30937	△○○	△△△△△	E(3541)
⋮	⋮	⋮	⋮	⋮

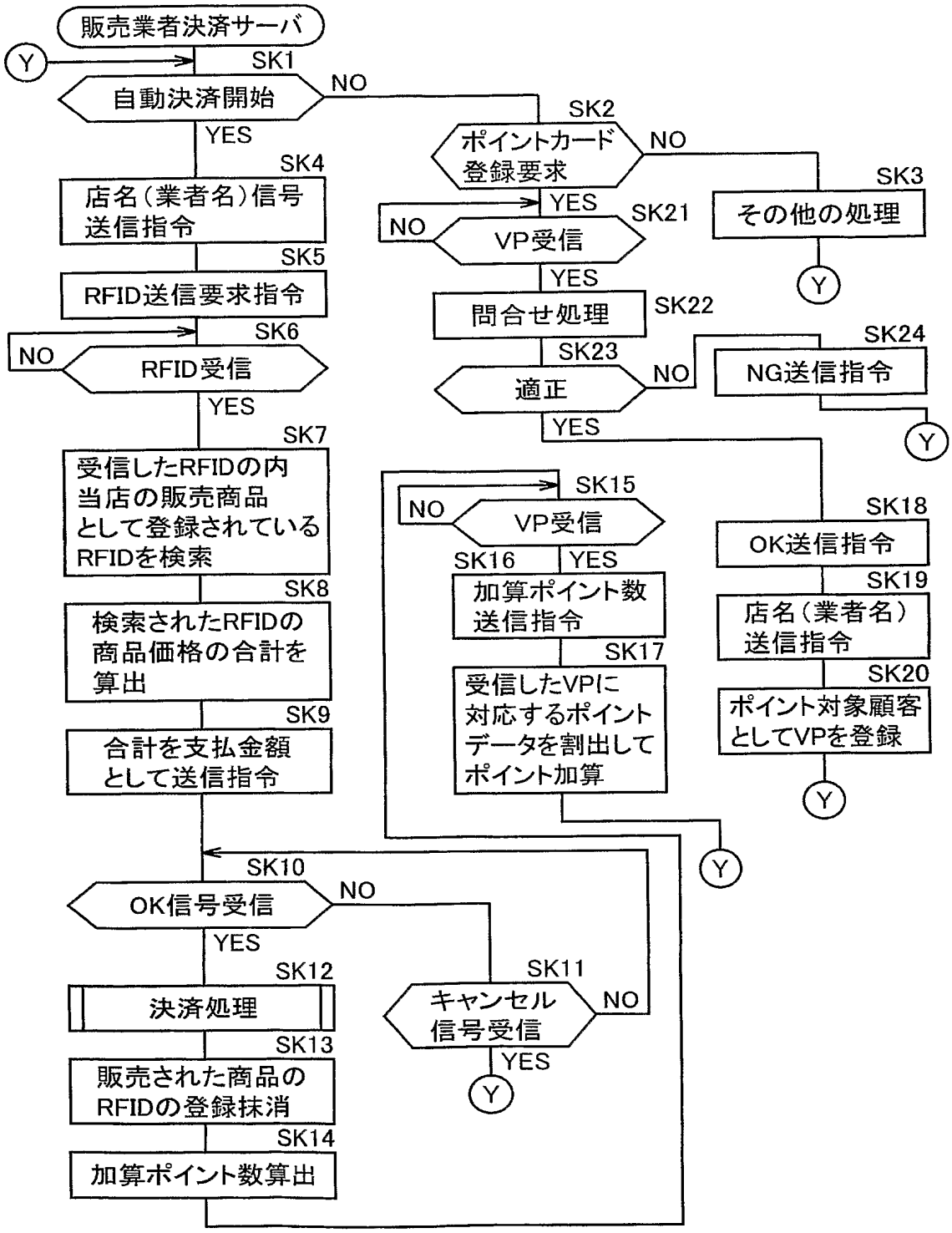
【図３１】


自動決済処理
SH1
自動決済開始信号受信
NO
RET
YES
SH2
NO
販売業者の店名信号受信
YES
SH3
YES
トラップ型RFIDあり
NO
SH4
業者名に対応させてトラップ型RFIDを記憶
SH5
NO
ポイントカード登録
YES
SH6
デビットカード決済，クレジットカード決済が可能な旨表示
SH7
支払金額受信処理
NO
決済種類入力操作あり
SH8
YES
SH9
支払金額表示
NO
OK操作あり
SH10
YES
SH11
NO
キャンセル操作あり
YES
SH12
キャンセル信号発信
RET
SH13
NO
リロード金額決済
YES
SH14
NO
支払金額≦リロード金額
YES
SH15
OK信号発信
SH16
VP用決済処理
C
SH17
ポイントカード加算処理
RET
SH18
キャンセル信号発信
SH19
残額不足表示
RET
SH20
NO
クレジット決済
YES
SH22
OK信号発信
SH23
VP用決済処理
C
SH21
デビット決済要求を発信
SH24
NO
OK信号受信
YES
SH25
VP用決済処理
C
SH26
NO
NG信号受信
YES
SH27
NG表示
RET

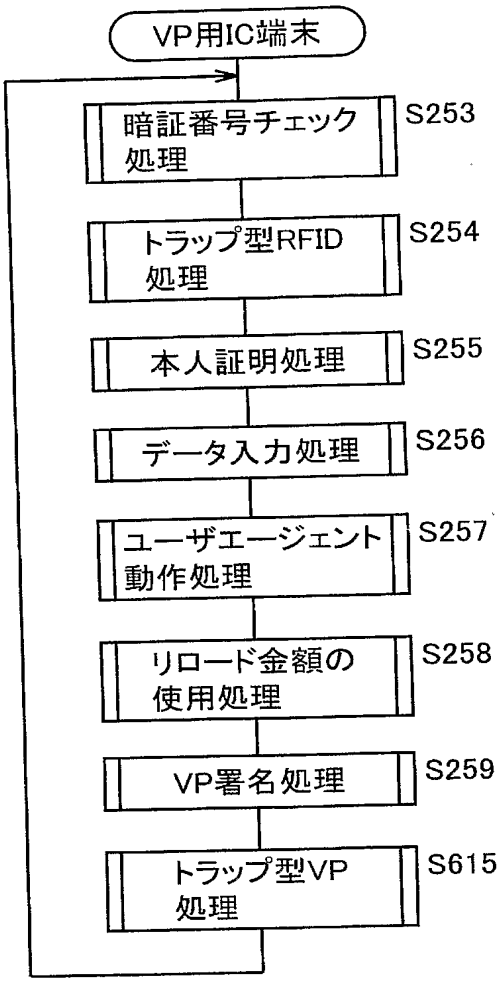
【図３２】


(a)
ポイントカード
加算処理
SI1
該当するVP発信
SI2
ポイント受信あり
NO
YES
SI3
該当する業者に
対応させて
ポイント加算記憶
RET
(b)
ポイントカード
登録処理
SJ1
ポイントカード
登録操作あり
NO
YES
RET
SJ2
既登録の
トラップ型
VP記憶あり
NO
YES
SJ3
トラップ型VPが
ない旨の表示
RET
SJ4
トラップ型VPを1つ
選択してその住所、
氏名等の必要情報を
発信
SJ5
OKを受信
NO
YES
SJ6
NGを受信
NO
YES
SJ7
NO
業者名受信
YES
SJ9
NG表示
SJ8
業者名に対応させて
トラップ型VPを記憶
RET

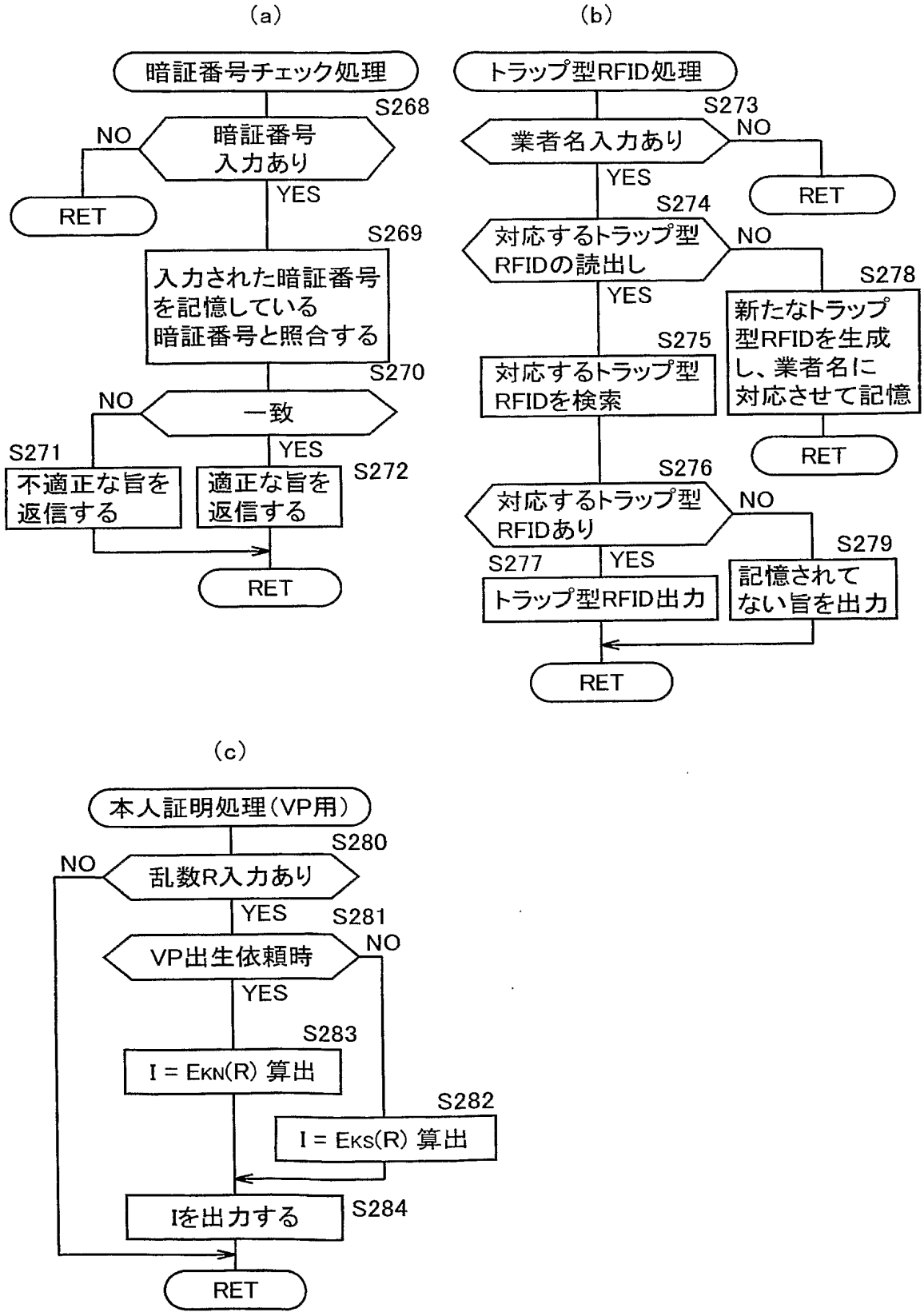
【図３３】


販売業者決済サーバ
Y
SK1
自動決済開始
NO
YES
SK2
ポイントカード登録要求
NO
YES
SK3
その他の処理
Y
SK4
店名（業者名）信号送信指令
SK5
RFID送信要求指令
SK6
NO
RFID受信
YES
SK7
受信したRFIDの内当店の販売商品として登録されているRFIDを検索
SK8
検索されたRFIDの商品価格の合計を算出
SK9
合計を支払金額として送信指令
SK10
OK信号受信
NO
YES
SK11
キャンセル信号受信
NO
YES
Y
SK12
決済処理
SK13
販売された商品のRFIDの登録抹消
SK14
加算ポイント数算出
SK21
NO
VP受信
YES
SK22
問合せ処理
SK23
適正
NO
YES
SK24
NG送信指令
Y
SK15
NO
VP受信
SK16
YES
加算ポイント数送信指令
SK17
受信したVPに対応するポイントデータを割出してポイント加算
Y
SK18
OK送信指令
SK19
店名（業者名）送信指令
SK20
ポイント対象顧客としてVPを登録
Y

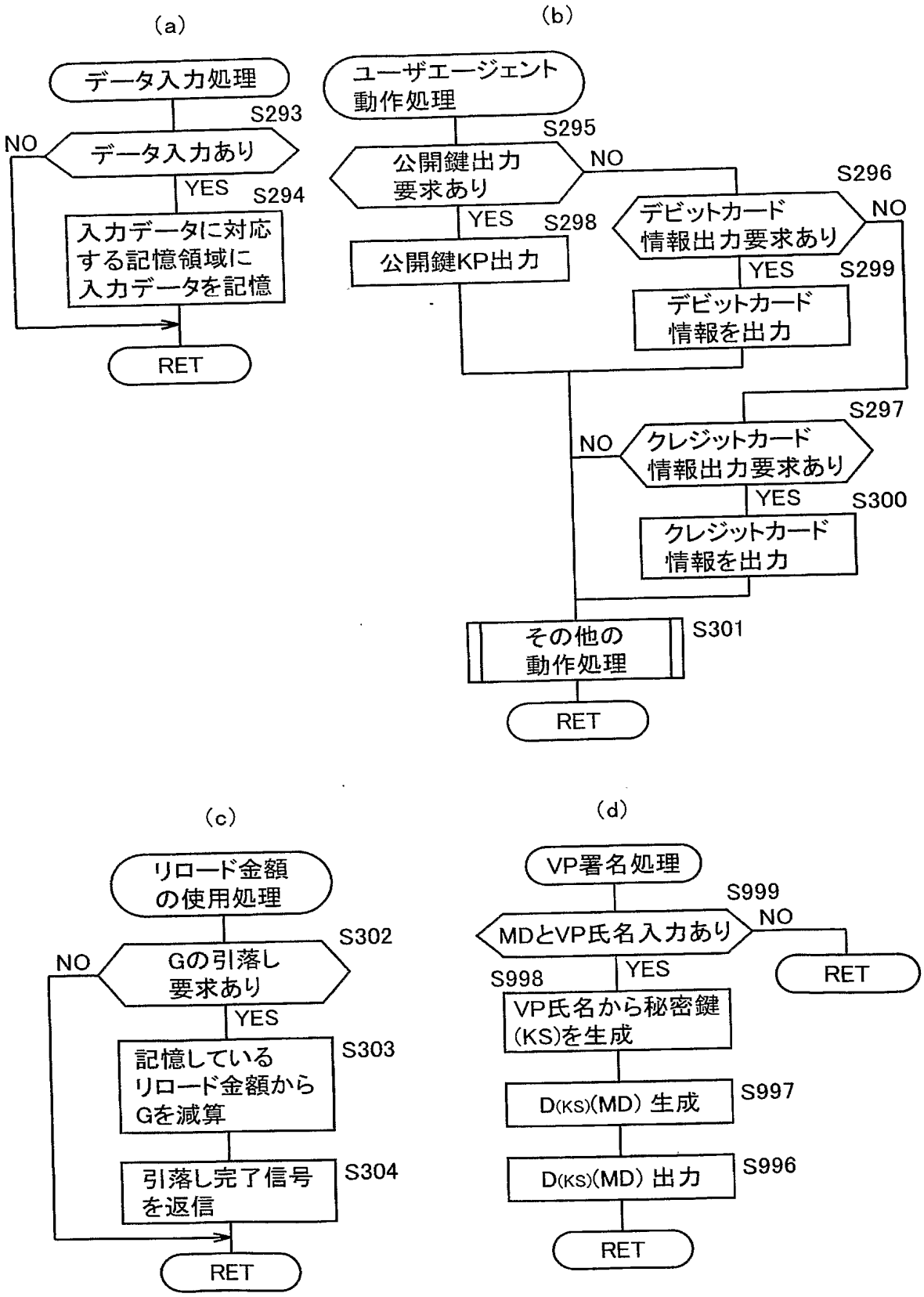
【図３４】


VP用IC端末
暗証番号チェック処理
S253
トラップ型RFID処理
S254
本人証明処理
S255
データ入力処理
S256
ユーザエージェント動作処理
S257
リロード金額の使用処理
S258
VP署名処理
S259
トラップ型VP処理
S615

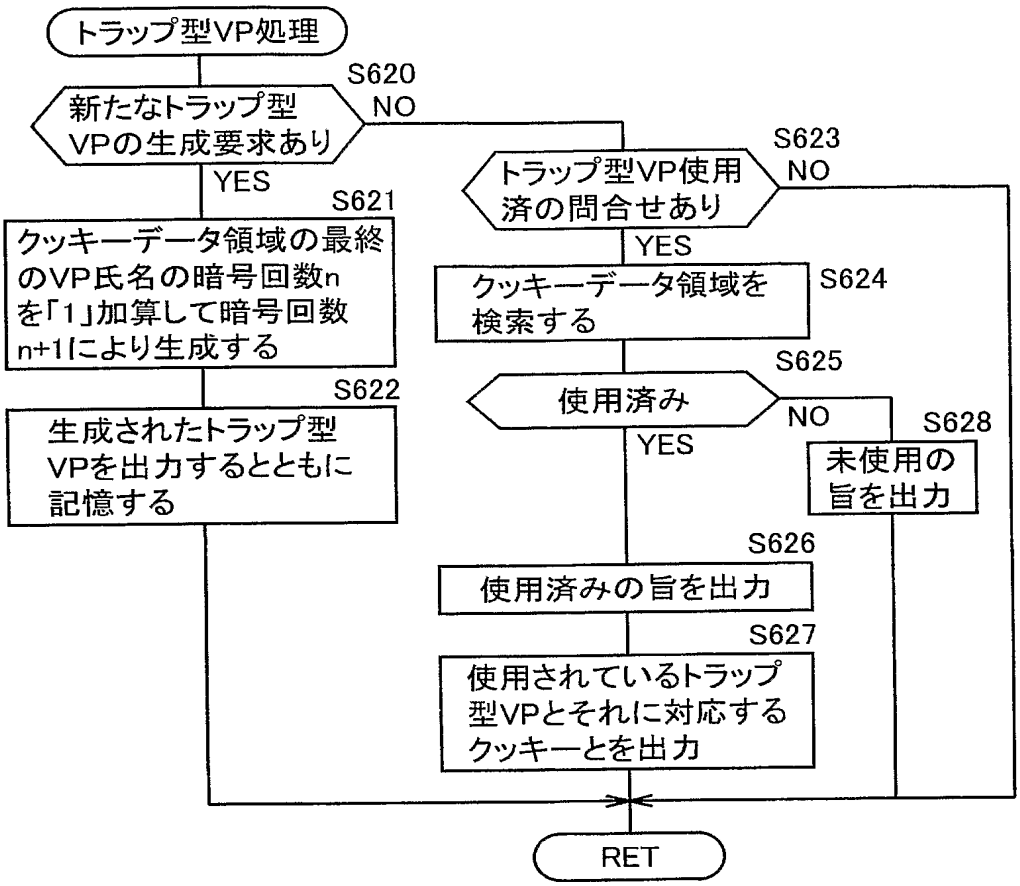
【図３５】


(a)
暗証番号チェック処理
S268
暗証番号
入力あり
NO
YES
RET
S269
入力された暗証番号
を記憶している
暗証番号と照合する
S270
一致
NO
YES
S271
不適正な旨を
返信する
S272
適正な旨を
返信する
RET
(b)
トラップ型RFID処理
S273
業者名入力あり
NO
YES
RET
S274
対応するトラップ型
RFIDの読出し
NO
YES
S278
新たなトラップ
型RFIDを生成
し、業者名に
対応させて記憶
S275
対応するトラップ型
RFIDを検索
RET
S276
対応するトラップ型
RFIDあり
NO
YES
S277
トラップ型RFID出力
S279
記憶されて
ない旨を出力
RET
(c)
本人証明処理(VP用)
S280
乱数R入力あり
NO
YES
S281
VP出生依頼時
NO
YES
S283
I = EKN(R) 算出
S282
I = EKS(R) 算出
Iを出力する
S284
RET

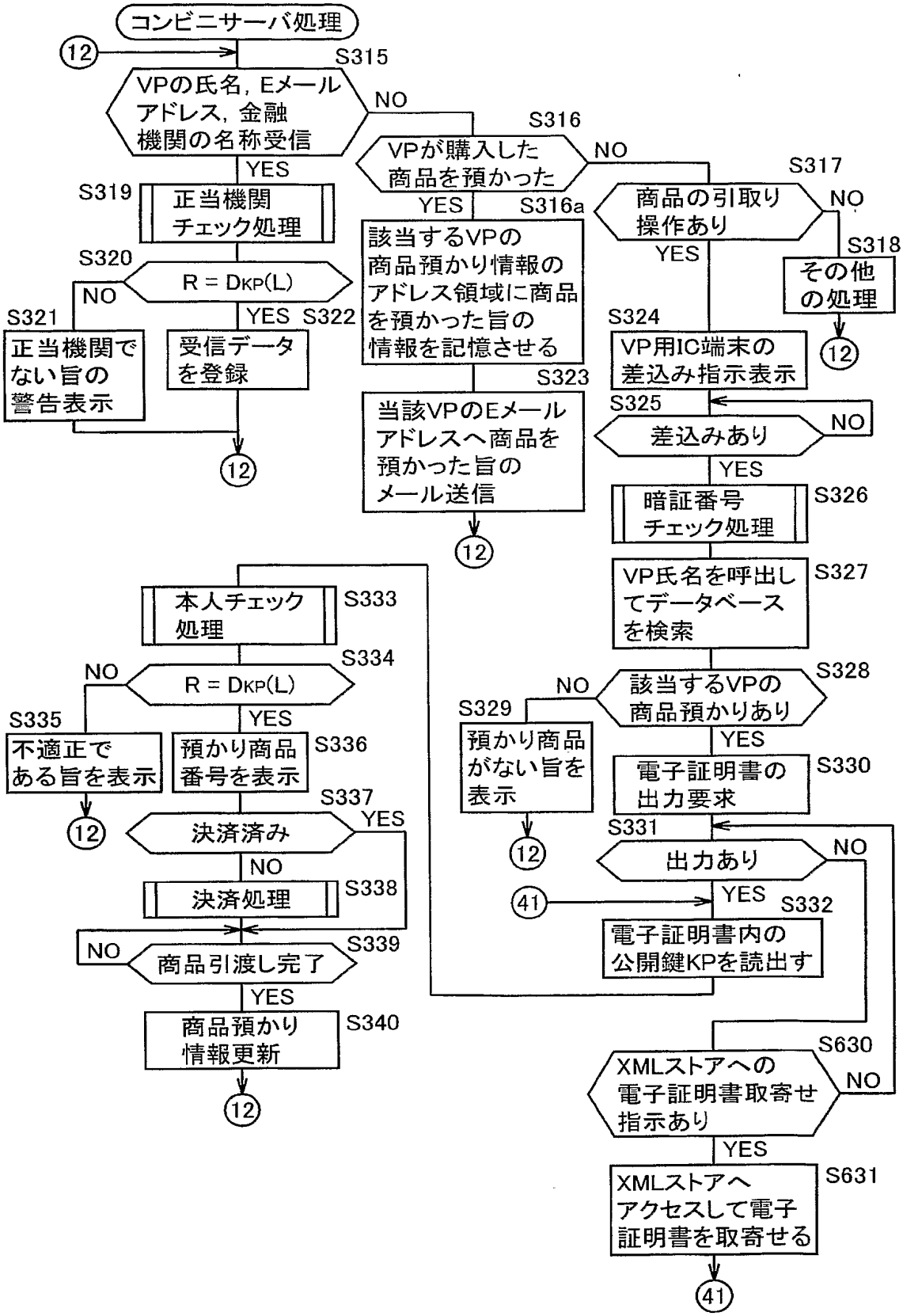
【図３６】


(a)
データ入力処理
S293
NO
データ入力あり
YES
S294
入力データに対応する記憶領域に入力データを記憶
RET
(b)
ユーザエージェント動作処理
S295
公開鍵出力要求あり
NO
S296
デビットカード情報出力要求あり
NO
YES
S298
公開鍵KP出力
YES
S299
デビットカード情報を出力
S297
NO
クレジットカード情報出力要求あり
YES
S300
クレジットカード情報を出力
その他の動作処理
S301
RET
(c)
リロード金額の使用処理
S302
NO
Gの引落し要求あり
YES
S303
記憶しているリロード金額からGを減算
S304
引落し完了信号を返信
RET
(d)
VP署名処理
S999
MDとVP氏名入力あり
NO
RET
S998
YES
VP氏名から秘密鍵(KS)を生成
D(KS)(MD) 生成
S997
D(KS)(MD) 出力
S996
RET

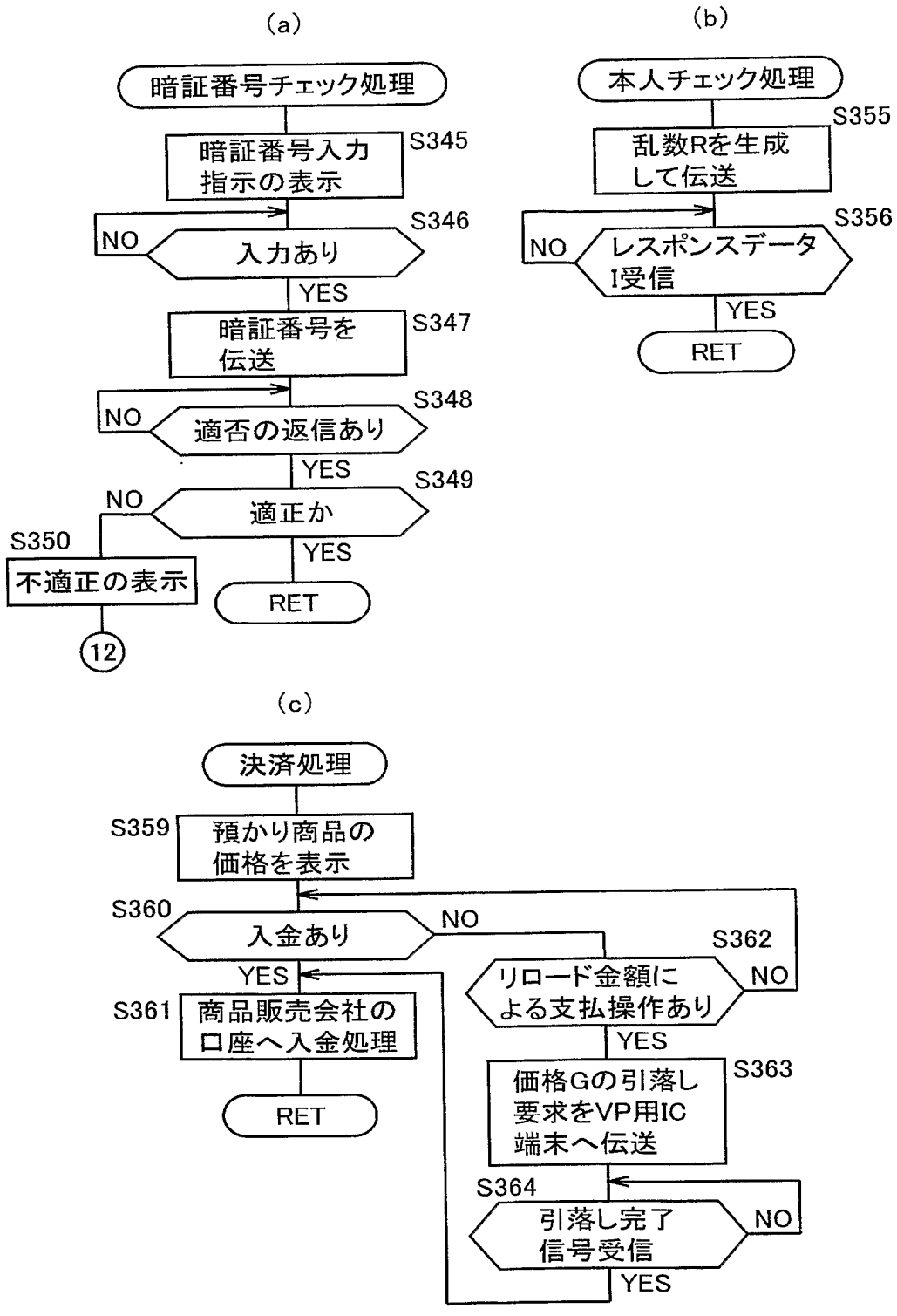
【図３７】


トラップ型VP処理
S620
新たなトラップ型VPの生成要求あり
NO
YES
S621
クッキーデータ領域の最終のVP氏名の暗号回数nを「1」加算して暗号回数n+1により生成する
S622
生成されたトラップ型VPを出力するとともに記憶する
S623
トラップ型VP使用済の問合せあり
NO
YES
S624
クッキーデータ領域を検索する
S625
使用済み
NO
S628
未使用の旨を出力
YES
S626
使用済みの旨を出力
S627
使用されているトラップ型VPとそれに対応するクッキーとを出力
RET

【図３８】


コンビニサーバ処理
12
S315
VPの氏名，Eメール
アドレス，金融
機関の名称受信
NO
YES
S316
VPが購入した
商品を預かった
NO
YES
S316a
該当するVPの
商品預かり情報の
アドレス領域に商品
を預かった旨の
情報を記憶させる
S317
商品の引取り
操作あり
NO
YES
S318
その他
の処理
12
S319
正当機関
チェック処理
S320
R = DKP(L)
NO
YES
S321
正当機関で
ない旨の
警告表示
S322
受信データ
を登録
12
S323
当該VPのEメール
アドレスへ商品を
預かった旨の
メール送信
12
S324
VP用IC端末の
差込み指示表示
S325
差込みあり
NO
YES
S326
暗証番号
チェック処理
S327
VP氏名を呼出し
てデータベース
を検索
S328
該当するVPの
商品預かりあり
NO
YES
S329
預かり商品
がない旨を
表示
12
S330
電子証明書の
出力要求
S331
出力あり
NO
YES
41
S332
電子証明書内の
公開鍵KPを読出す
S333
本人チェック
処理
S334
R = DKP(L)
NO
YES
S335
不適正で
ある旨を表示
12
S336
預かり商品
番号を表示
S337
決済済み
YES
NO
S338
決済処理
NO
S339
商品引渡し完了
YES
S340
商品預かり
情報更新
12
S630
XMLストアへの
電子証明書取寄せ
指示あり
NO
YES
S631
XMLストアへ
アクセスして電子
証明書を取寄せる
41

【図３９】

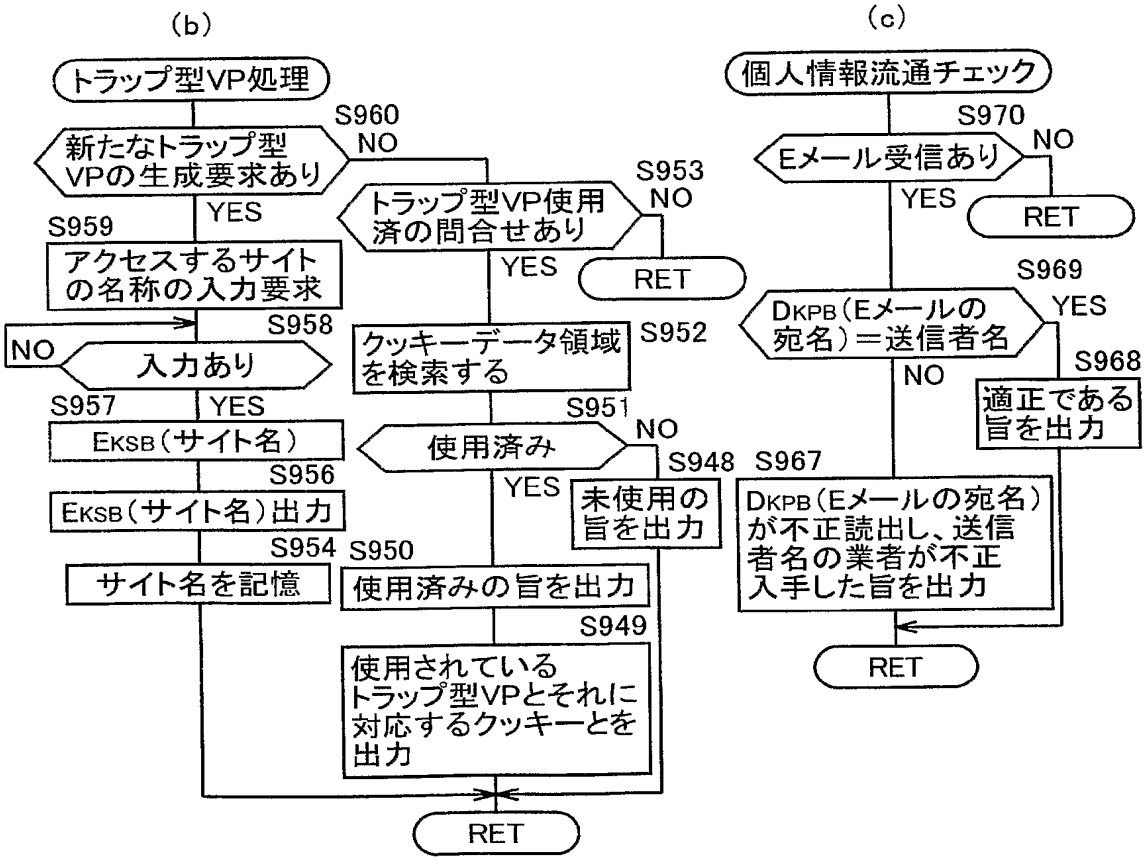

(a)
暗証番号チェック処理
暗証番号入力指示の表示
S345
NO
入力あり
S346
YES
暗証番号を伝送
S347
NO
適否の返信あり
S348
YES
適正か
S349
NO
S350
不適正の表示
YES
RET
12
(b)
本人チェック処理
乱数Rを生成して伝送
S355
NO
レスポンスデータI受信
S356
YES
RET
(c)
決済処理
S359
預かり商品の価格を表示
S360
入金あり
NO
S362
リロード金額による支払操作あり
NO
YES
S361
商品販売会社の口座へ入金処理
RET
YES
価格Gの引落し要求をVP用IC端末へ伝送
S363
S364
引落し完了信号受信
NO
YES

【図４０】

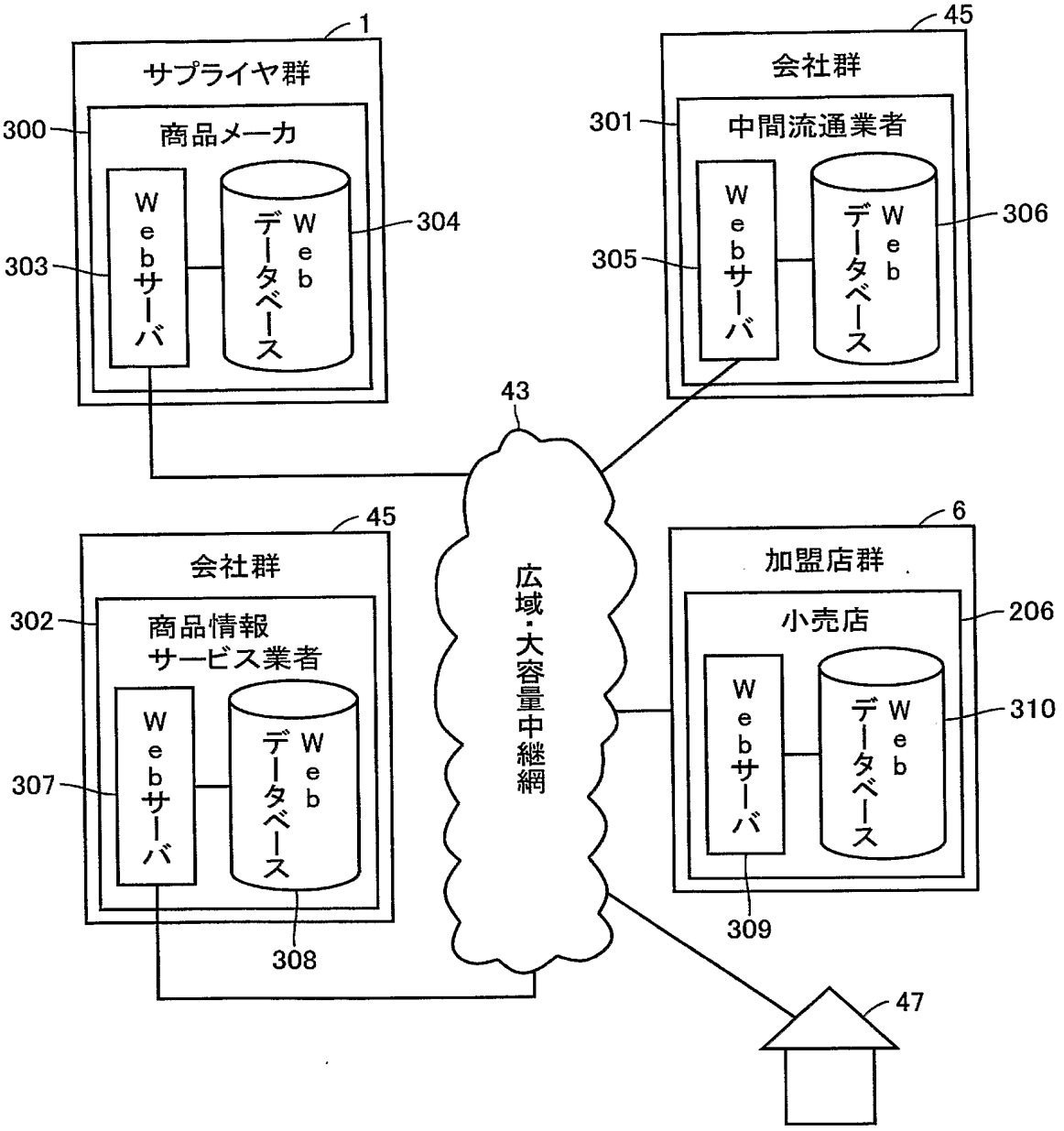
(a)

トラップ型ＲＦＩＤ

VP氏名	トラップ型RFID	業者名
B13P	abc,hij,amz,rak・・・	ABC,HIJ,AMZ・・・
E_{KSB}（各サイト名）	mtt	MTT
	mec	MEC
	ktt	KTT
	⋮	⋮



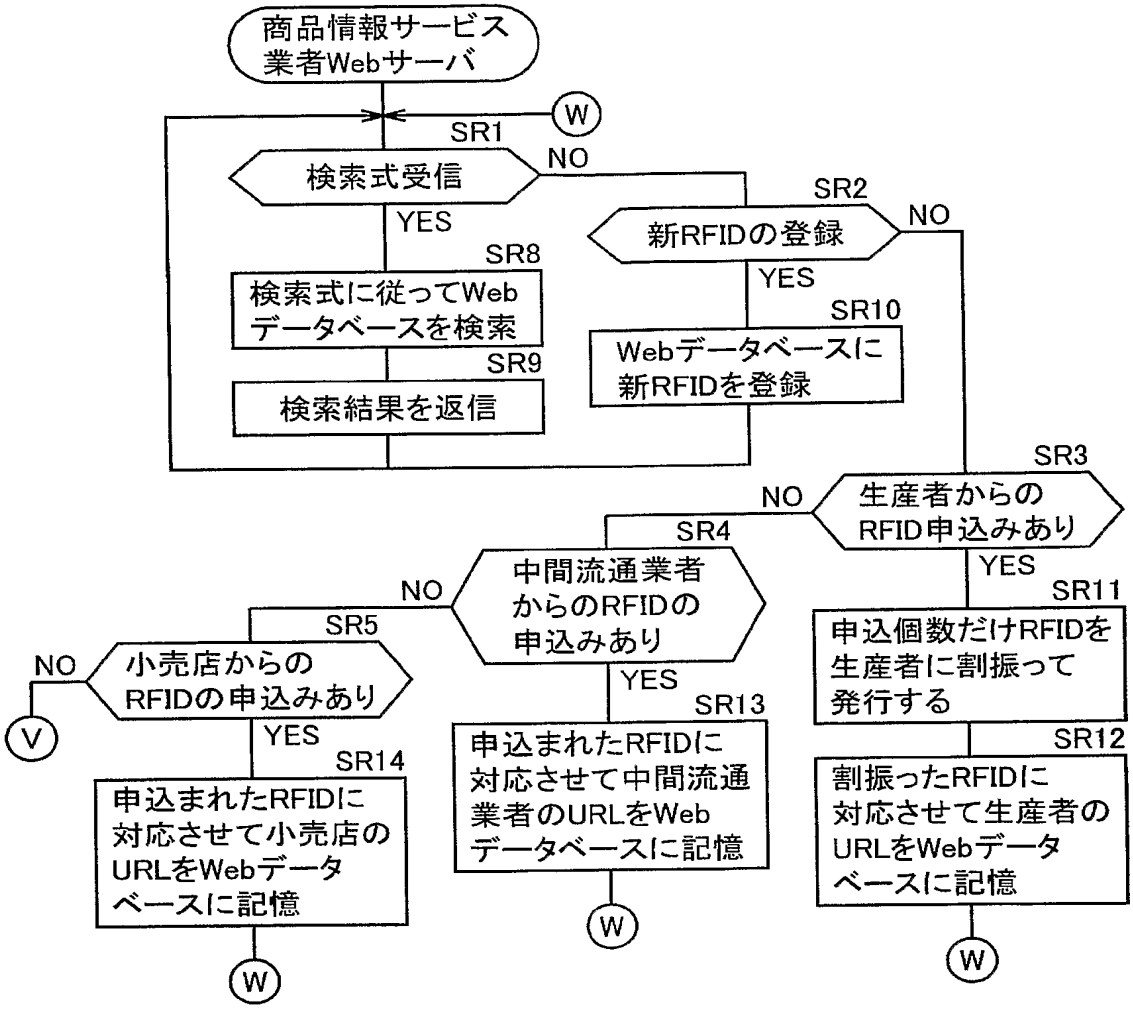
【図４１】


1
サプライヤ群
300
商品メーカ
303
Webサーバ
Web
データベース
304
45
会社群
301
中間流通業者
305
Webサーバ
Web
データベース
306
43
広域・大容量中継網
45
会社群
302
商品情報
サービス業者
307
Webサーバ
Web
データベース
308
6
加盟店群
206
小売店
Webサーバ
Web
データベース
310
309
47

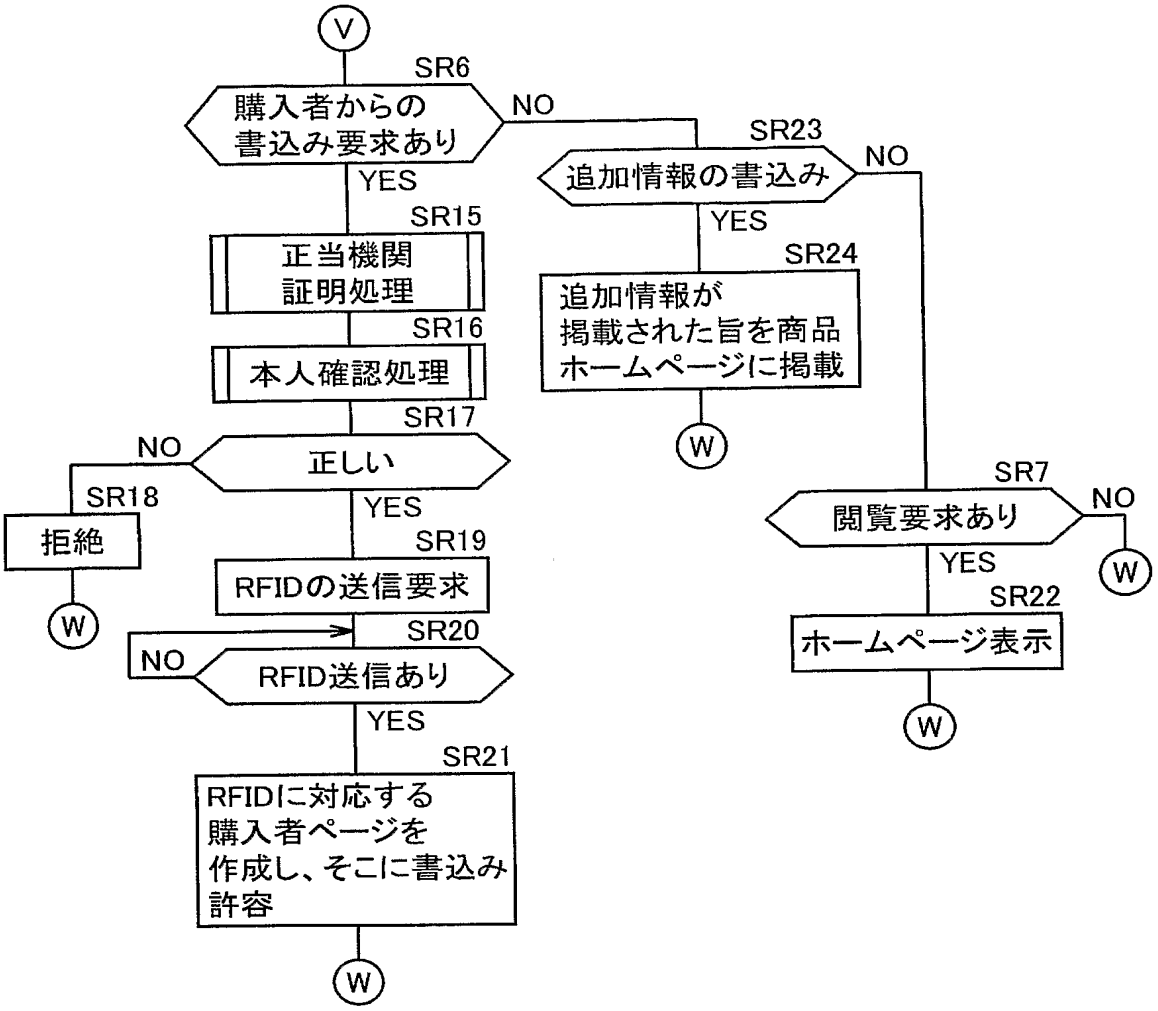
【図４２】

RFID	生産者	中間流通業者	小売店	購入者ページ		
892013960	http//www.sato	http//www.kanei	http//www.daimaru	B13P	・・・	・・・
892013961				NPXA	・・・	・・・
892013962 ～ 892014560				I9X3	・・・	・・・
892014561 ～ 892014801	http//www.isida		http//www.hansin			
892014802 ～ 892014990	http//www.kato	http//www.mitui				

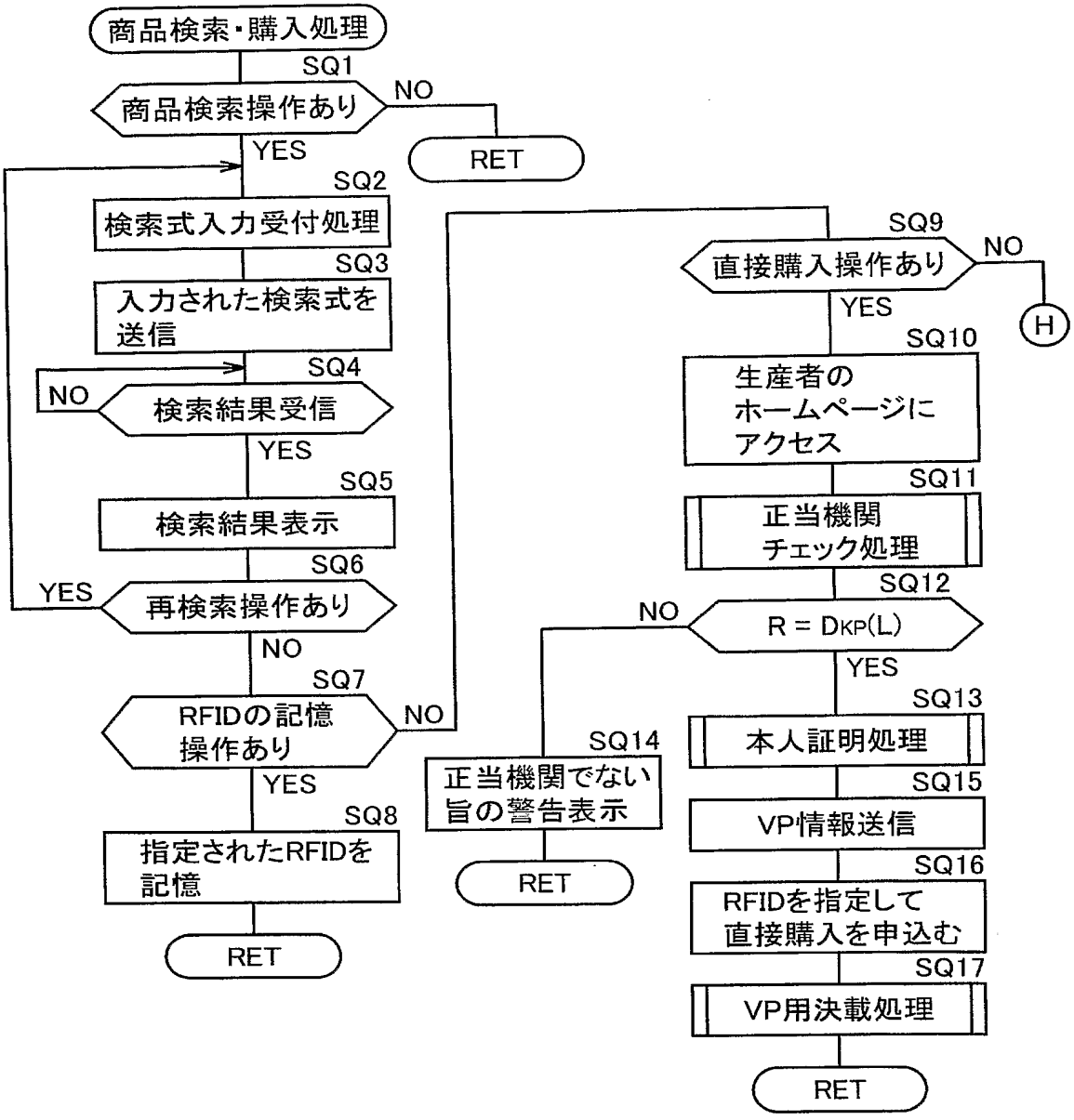
【図４３】


商品情報サービス
業者Webサーバ
W
SR1
検索式受信
NO
YES
SR2
新RFIDの登録
NO
YES
SR8
検索式に従ってWeb
データベースを検索
SR9
検索結果を返信
SR10
Webデータベースに
新RFIDを登録
SR3
生産者からの
RFID申込みあり
NO
YES
SR4
中間流通業者
からのRFIDの
申込みあり
NO
YES
SR11
申込個数だけRFIDを
生産者に割振って
発行する
SR5
小売店からの
RFIDの申込みあり
NO
YES
V
SR14
申込まれたRFIDに
対応させて小売店の
URLをWebデータ
ベースに記憶
SR13
申込まれたRFIDに
対応させて中間流通
業者のURLをWeb
データベースに記憶
SR12
割振ったRFIDに
対応させて生産者の
URLをWebデータ
ベースに記憶
W
W
W

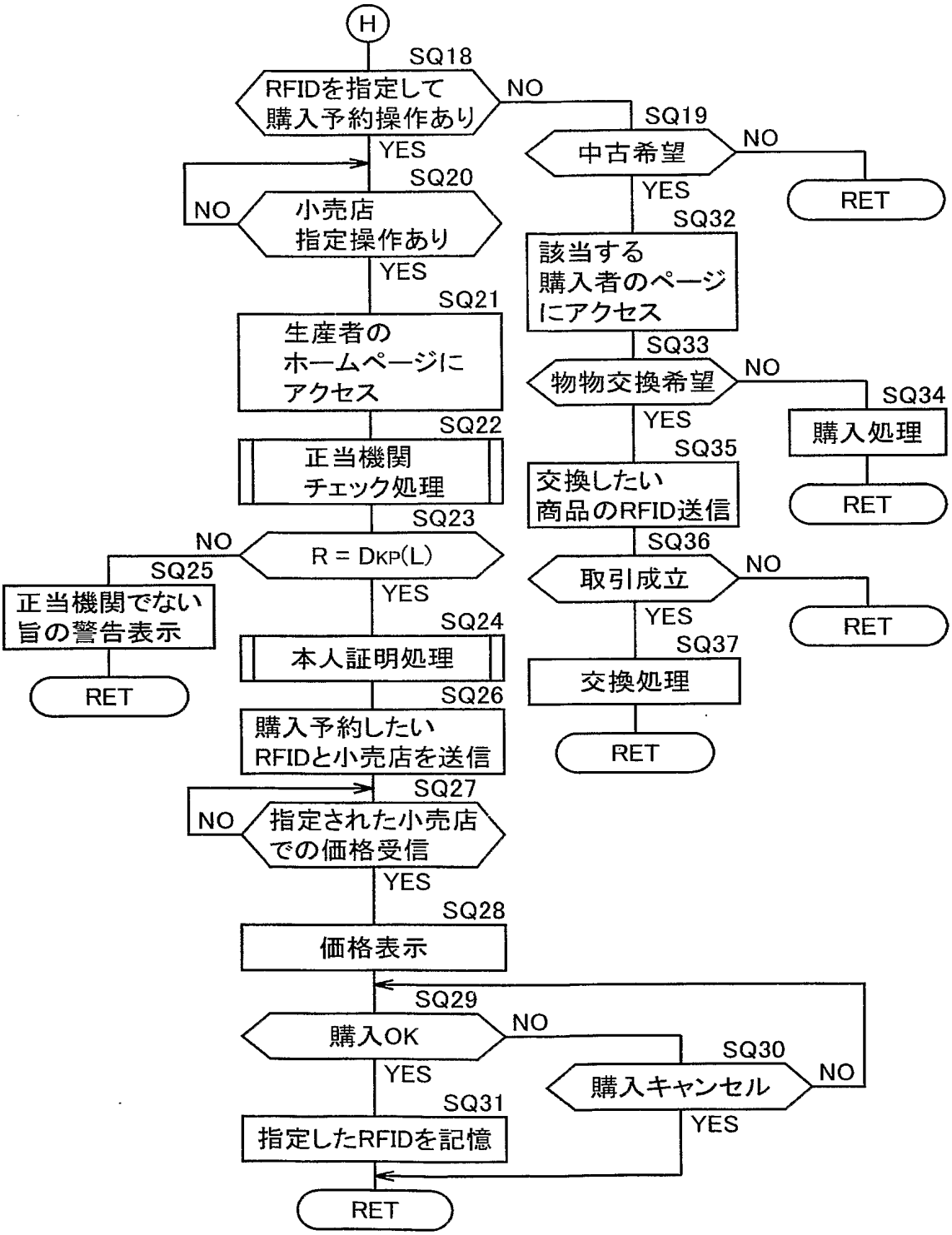
【図４４】


V
SR6
購入者からの
書込み要求あり
NO
YES
SR15
正当機関
証明処理
SR16
本人確認処理
SR17
正しい
NO
YES
SR18
拒絶
W
SR19
RFIDの送信要求
SR20
NO
RFID送信あり
YES
SR21
RFIDに対応する
購入者ページを
作成し、そこに書込み
許容
W
SR23
追加情報の書込み
NO
YES
SR24
追加情報が
掲載された旨を商品
ホームページに掲載
W
SR7
閲覧要求あり
NO
W
YES
SR22
ホームページ表示
W

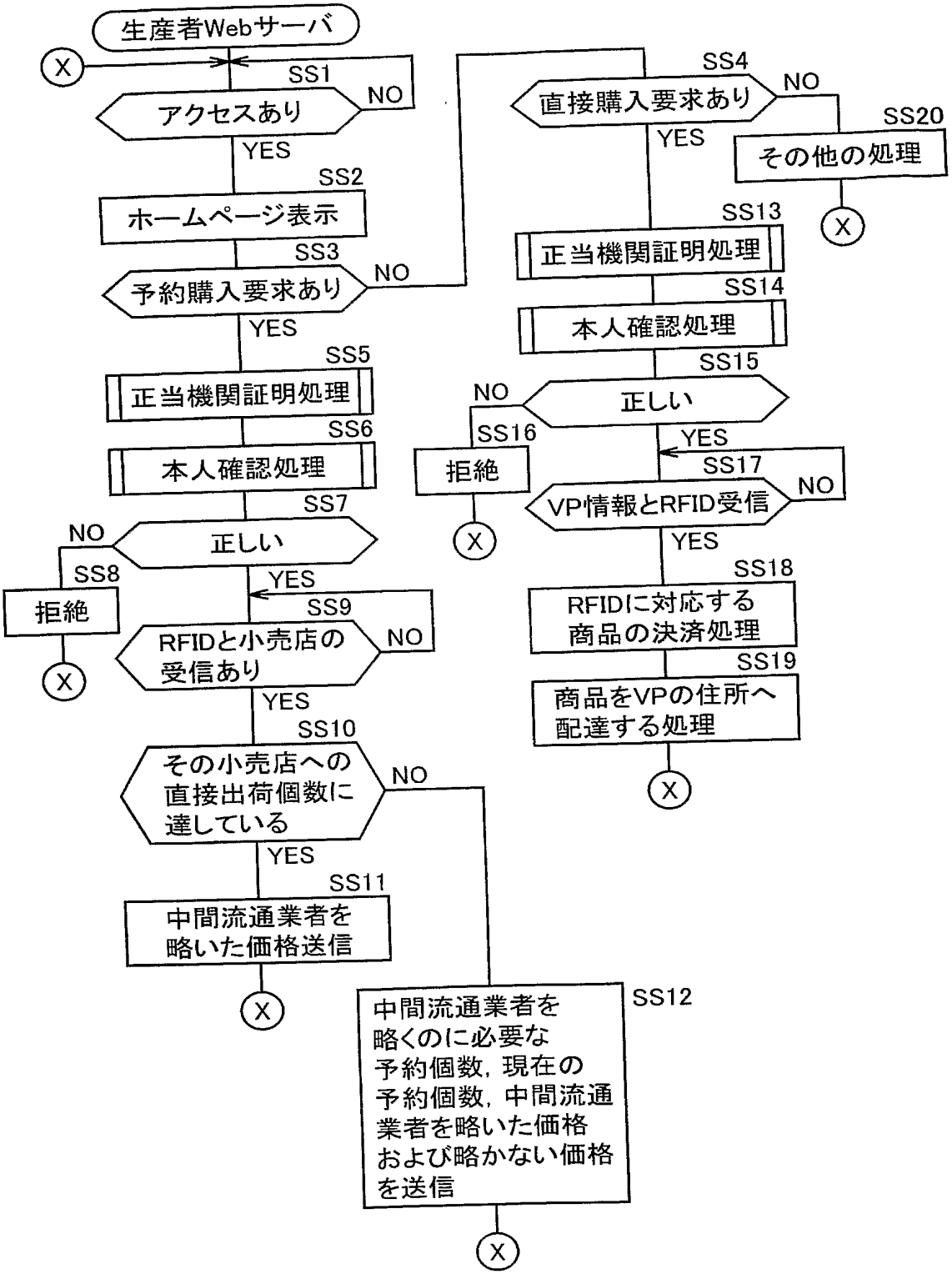
【図４５】


商品検索・購入処理
SQ1
商品検索操作あり
NO
RET
YES
SQ2
検索式入力受付処理
SQ3
入力された検索式を送信
SQ4
NO
検索結果受信
YES
SQ5
検索結果表示
SQ6
YES
再検索操作あり
NO
SQ7
RFIDの記憶操作あり
NO
YES
SQ8
指定されたRFIDを記憶
RET
SQ9
直接購入操作あり
NO
H
YES
SQ10
生産者のホームページにアクセス
SQ11
正当機関チェック処理
SQ12
NO
R = DKP(L)
YES
SQ13
本人証明処理
SQ14
正当機関でない旨の警告表示
RET
SQ15
VP情報送信
SQ16
RFIDを指定して直接購入を申込む
SQ17
VP用決載処理
RET

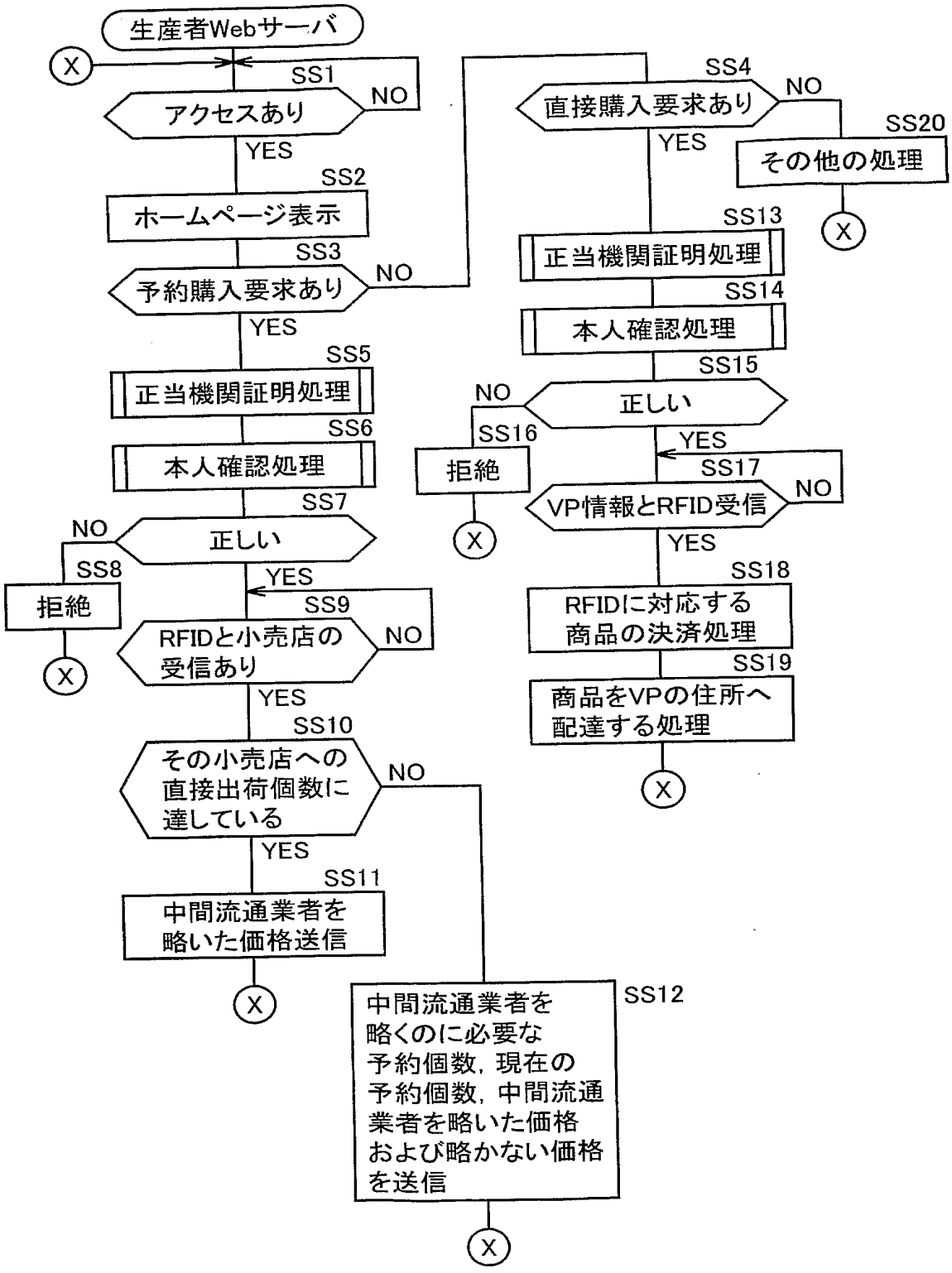
【図４６】


H
SQ18
RFIDを指定して
購入予約操作あり
NO
YES
SQ19
中古希望
NO
RET
YES
SQ20
NO
小売店
指定操作あり
YES
SQ32
該当する
購入者のページ
にアクセス
SQ21
生産者の
ホームページに
アクセス
SQ33
物物交換希望
NO
SQ34
購入処理
RET
YES
SQ22
正当機関
チェック処理
SQ35
交換したい
商品のRFID送信
SQ23
NO
R = DKP(L)
SQ36
取引成立
NO
RET
SQ25
正当機関でない
旨の警告表示
YES
SQ24
本人証明処理
YES
SQ37
交換処理
RET
RET
SQ26
購入予約したい
RFIDと小売店を送信
SQ27
NO
指定された小売店
での価格受信
YES
SQ28
価格表示
SQ29
購入OK
NO
SQ30
購入キャンセル
NO
YES
YES
SQ31
指定したRFIDを記憶
RET

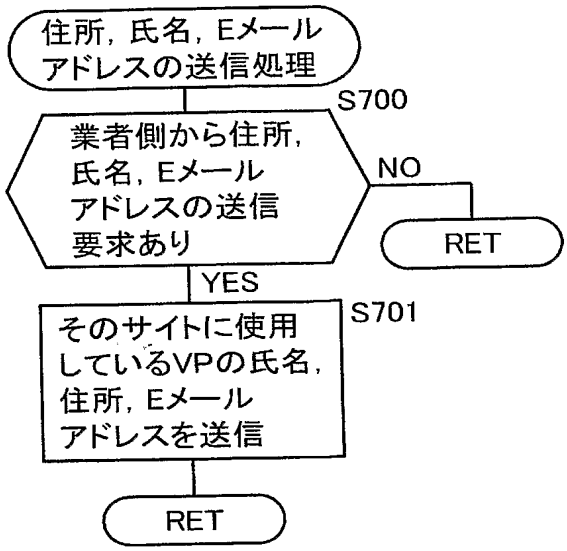
【図４７】


生産者Webサーバ
X
SS1
アクセスあり
NO
YES
SS2
ホームページ表示
SS3
予約購入要求あり
NO
YES
SS5
正当機関証明処理
SS6
本人確認処理
SS7
正しい
NO
SS8
拒絶
X
YES
SS9
RFIDと小売店の受信あり
NO
YES
SS10
その小売店への直接出荷個数に達している
NO
YES
SS11
中間流通業者を略いた価格送信
X
SS12
中間流通業者を略くのに必要な予約個数，現在の予約個数，中間流通業者を略いた価格および略かない価格を送信
X
SS4
直接購入要求あり
NO
YES
SS20
その他の処理
X
SS13
正当機関証明処理
SS14
本人確認処理
SS15
正しい
NO
SS16
拒絶
X
YES
SS17
VP情報とRFID受信
NO
YES
SS18
RFIDに対応する商品の決済処理
SS19
商品をVPの住所へ配達する処理
X

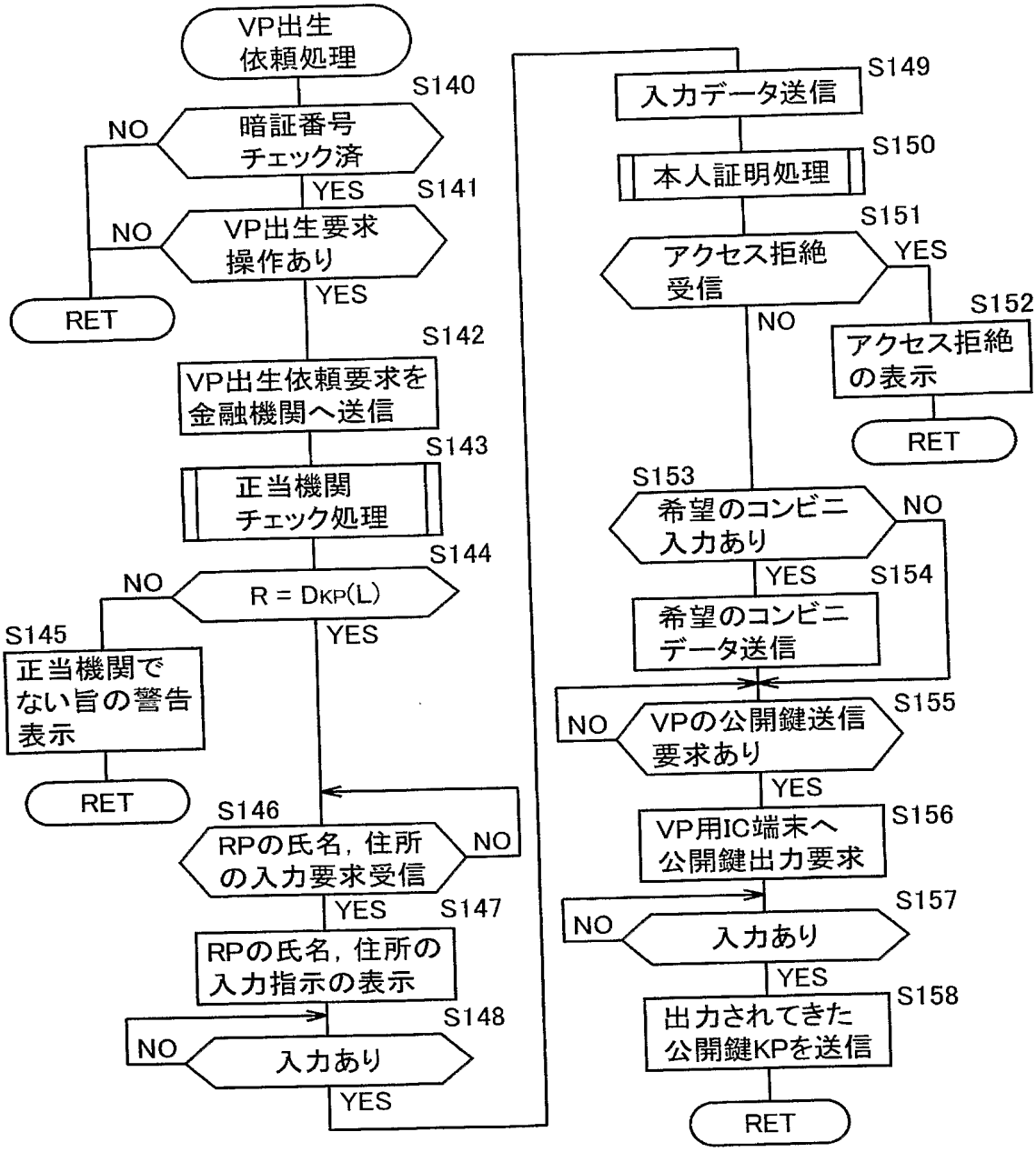
【図４７】


生産者Webサーバ
X
SS1
アクセスあり
NO
YES
SS2
ホームページ表示
SS3
予約購入要求あり
NO
YES
SS5
正当機関証明処理
SS6
本人確認処理
SS7
正しい
NO
SS8
拒絶
X
YES
SS9
RFIDと小売店の受信あり
NO
YES
SS10
その小売店への直接出荷個数に達している
NO
YES
SS11
中間流通業者を略いた価格送信
X
SS12
中間流通業者を略くのに必要な予約個数，現在の予約個数，中間流通業者を略いた価格および略かない価格を送信
X
SS4
直接購入要求あり
NO
YES
SS20
その他の処理
X
SS13
正当機関証明処理
SS14
本人確認処理
SS15
正しい
NO
SS16
拒絶
X
YES
SS17
VP情報とRFID受信
NO
YES
SS18
RFIDに対応する商品の決済処理
SS19
商品をVPの住所へ配達する処理
X

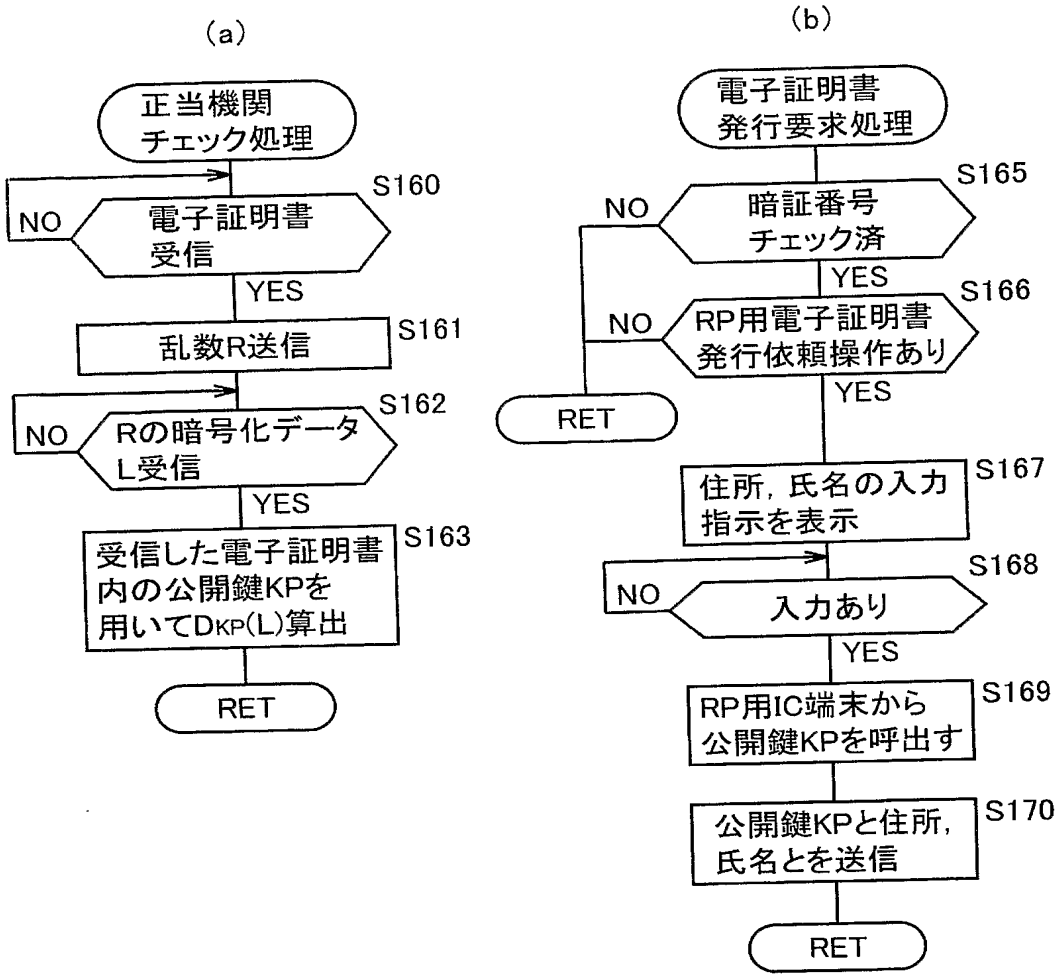
【図４８】


住所，氏名，Eメール
アドレスの送信処理
S700
業者側から住所，
氏名，Eメール
アドレスの送信
要求あり
NO
RET
YES
S701
そのサイトに使用
しているVPの氏名，
住所，Eメール
アドレスを送信
RET

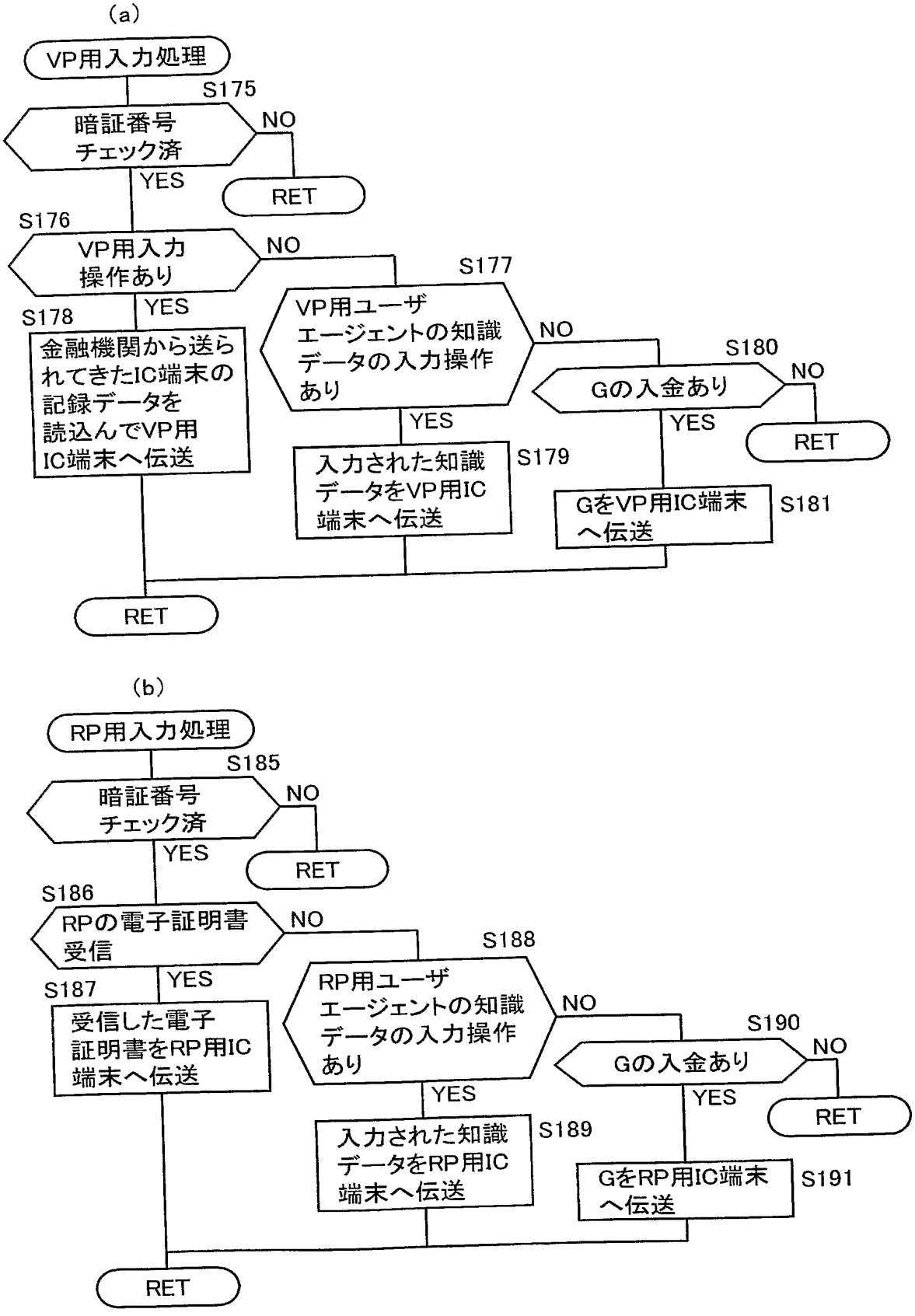
【図４９】


VP出生
依頼処理
S140
暗証番号
チェック済
NO
YES
S141
VP出生要求
操作あり
NO
YES
RET
S142
VP出生依頼要求を
金融機関へ送信
S143
正当機関
チェック処理
S144
R = DKP(L)
NO
YES
S145
正当機関で
ない旨の警告
表示
RET
S146
RPの氏名，住所
の入力要求受信
NO
YES
S147
RPの氏名，住所の
入力指示の表示
S148
入力あり
NO
YES
S149
入力データ送信
S150
本人証明処理
S151
アクセス拒絶
受信
YES
NO
S152
アクセス拒絶
の表示
RET
S153
希望のコンビニ
入力あり
NO
YES
S154
希望のコンビニ
データ送信
S155
VPの公開鍵送信
要求あり
NO
YES
S156
VP用IC端末へ
公開鍵出力要求
S157
入力あり
NO
YES
S158
出力されてきた
公開鍵KPを送信
RET

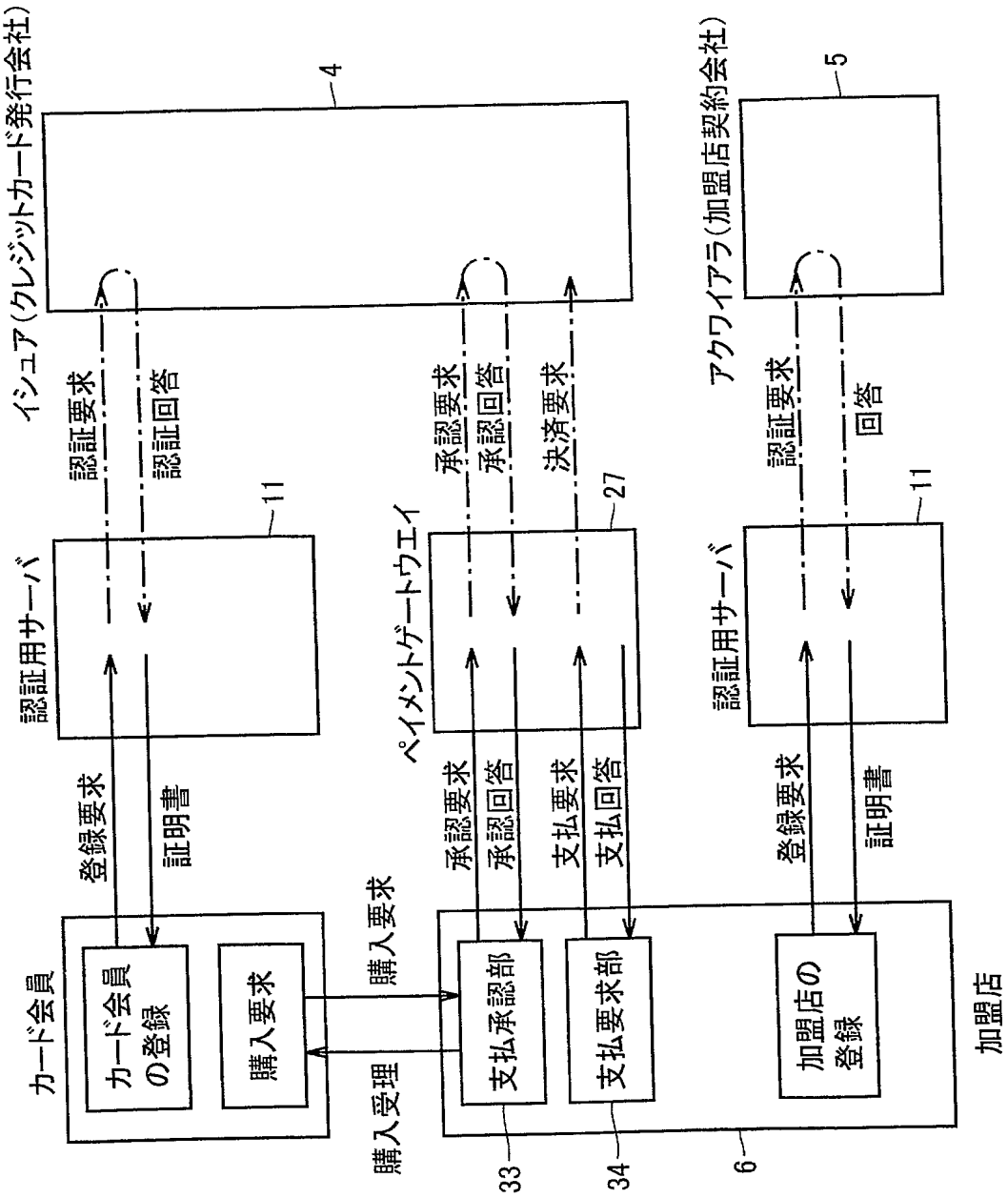
【図５０】


(a)
正当機関
チェック処理
S160
NO
電子証明書
受信
YES
乱数R送信
S161
S162
NO
Rの暗号化データ
L受信
YES
受信した電子証明書
内の公開鍵KPを
用いてDKP(L)算出
S163
RET
(b)
電子証明書
発行要求処理
S165
NO
暗証番号
チェック済
YES
S166
NO
RP用電子証明書
発行依頼操作あり
YES
RET
住所，氏名の入力
指示を表示
S167
S168
NO
入力あり
YES
RP用IC端末から
公開鍵KPを呼出す
S169
公開鍵KPと住所，
氏名とを送信
S170
RET

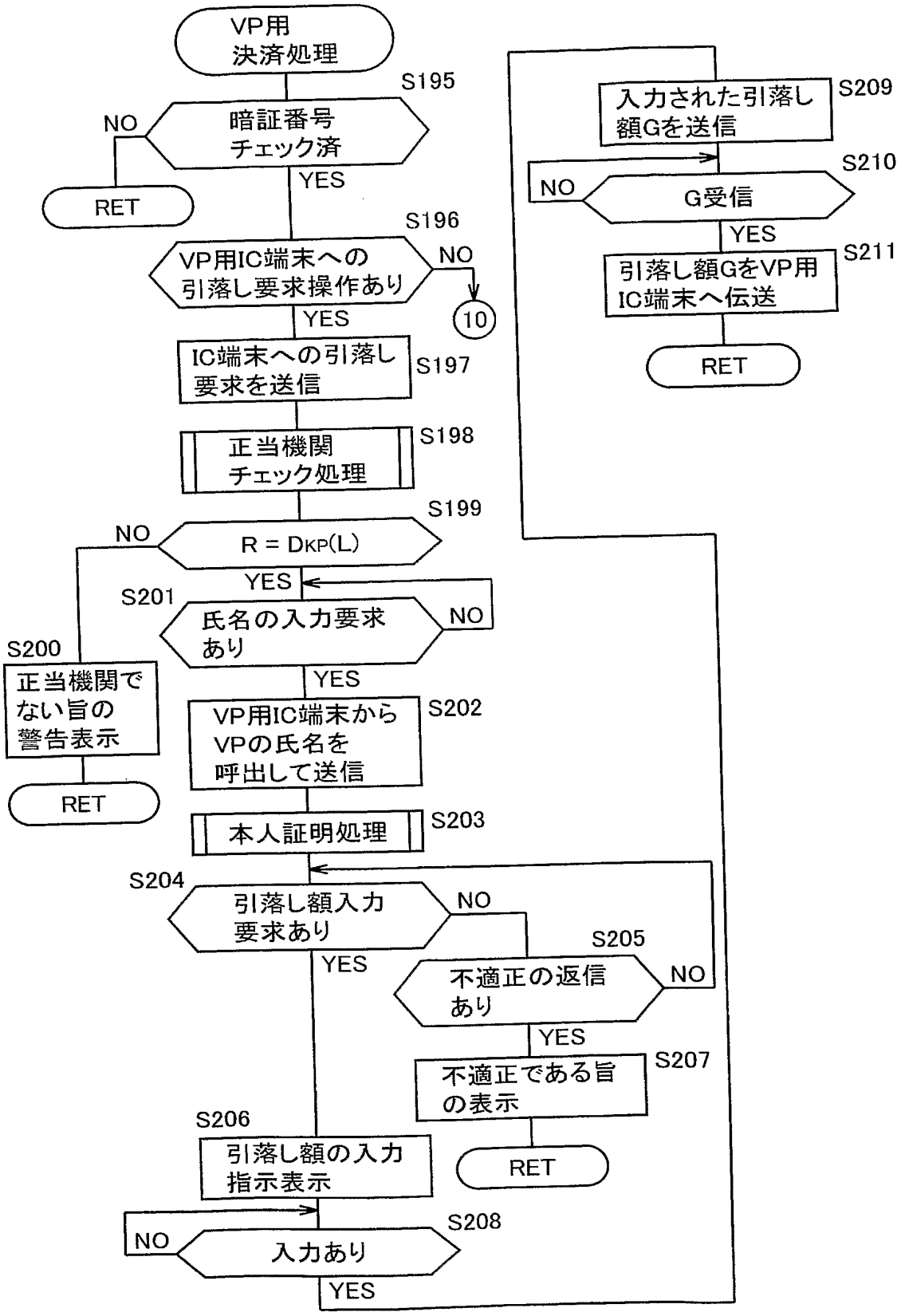
【図５１】


(a)
VP用入力処理
S175
暗証番号チェック済
NO
RET
YES
S176
VP用入力操作あり
NO
S177
VP用ユーザエージェントの知識データの入力操作あり
YES
S178
金融機関から送られてきたIC端末の記録データを読込んでVP用IC端末へ伝送
NO
S180
Gの入金あり
NO
RET
YES
入力された知識データをVP用IC端末へ伝送
S179
GをVP用IC端末へ伝送
S181
RET
(b)
RP用入力処理
S185
暗証番号チェック済
NO
RET
YES
S186
RPの電子証明書受信
NO
S188
RP用ユーザエージェントの知識データの入力操作あり
YES
S187
受信した電子証明書をRP用IC端末へ伝送
NO
S190
Gの入金あり
NO
RET
YES
入力された知識データをRP用IC端末へ伝送
S189
GをRP用IC端末へ伝送
S191
RET

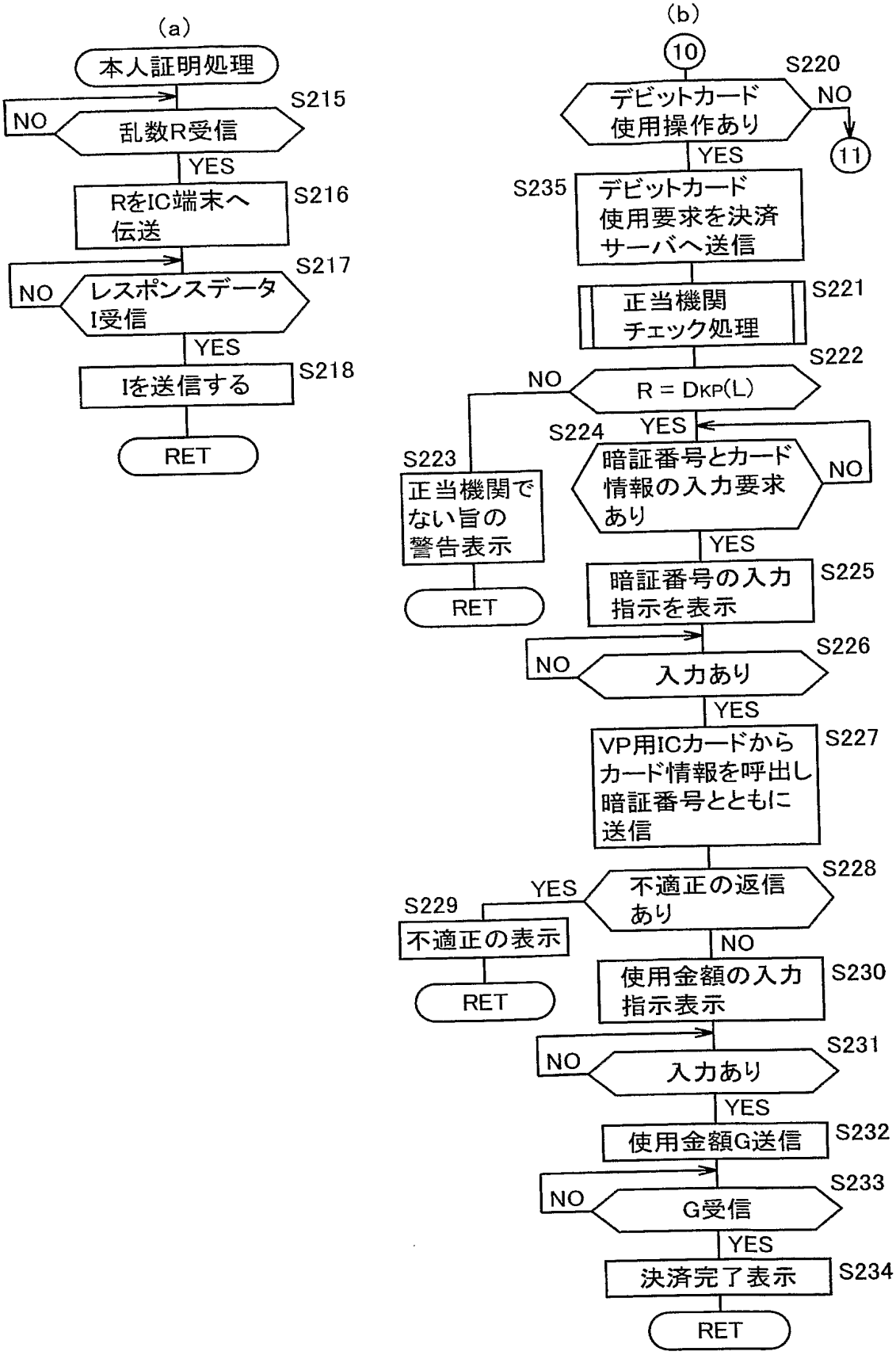
【図５２】


イシュア（クレジットカード発行会社）
4
認証要求
認証回答
認証用サーバ
11
登録要求
証明書
カード会員
カード会員の登録
購入要求
購入要求
購入受理
ペイメントゲートウエイ
27
承認要求
承認回答
決済要求
承認要求
承認回答
支払要求
支払回答
支払承認部
支払要求部
33
34
アクワイアラ（加盟店契約会社）
5
認証要求
回答
認証用サーバ
11
登録要求
証明書
加盟店の登録
6
加盟店

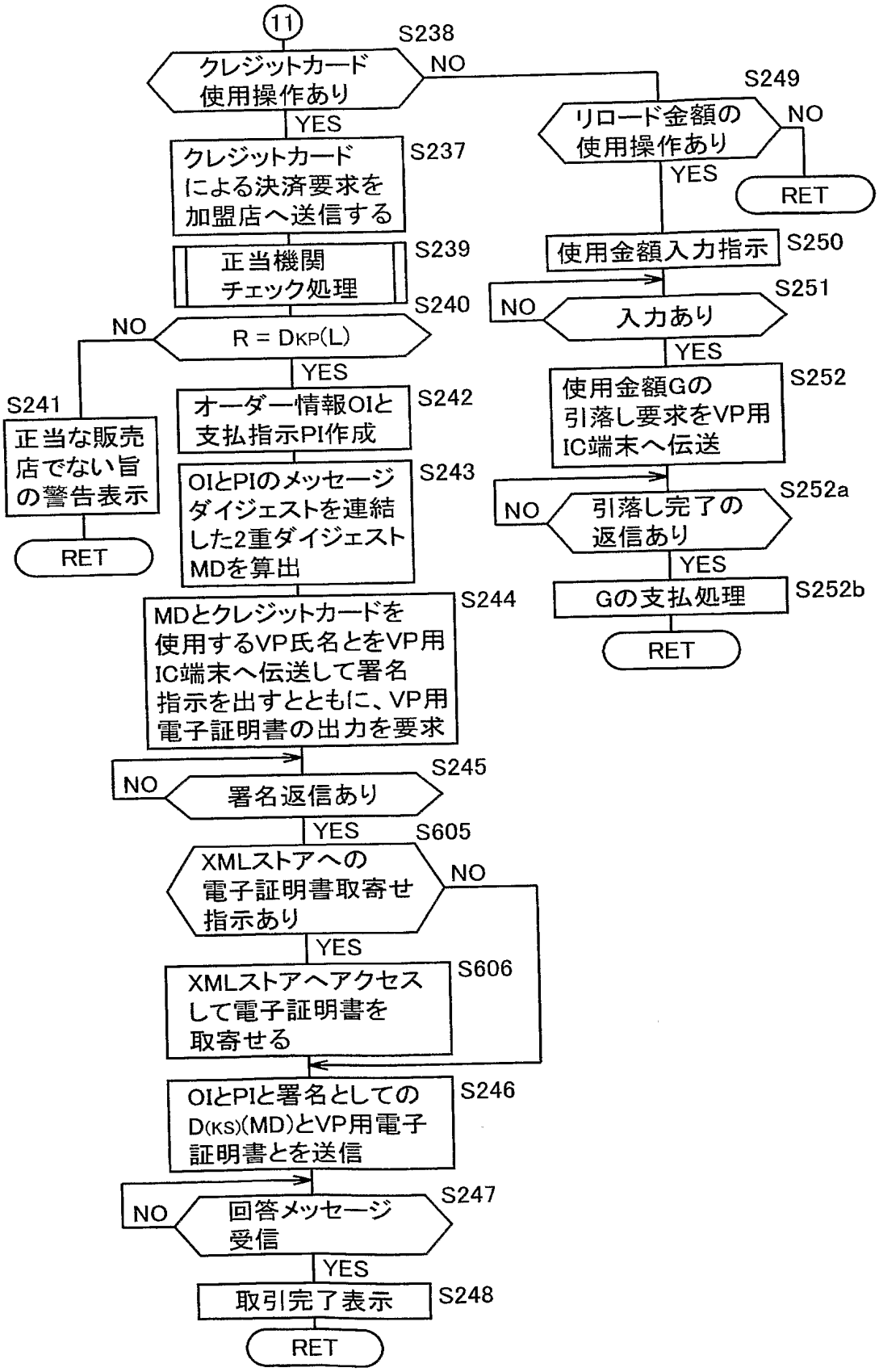
【図５３】


VP用
決済処理
S195
暗証番号
チェック済
NO
YES
RET
S196
VP用IC端末への
引落し要求操作あり
NO
YES
10
IC端末への引落し
要求を送信
S197
正当機関
チェック処理
S198
S199
R = DKP(L)
NO
YES
S201
氏名の入力要求
あり
NO
YES
S200
正当機関で
ない旨の
警告表示
RET
VP用IC端末から
VPの氏名を
呼出して送信
S202
本人証明処理
S203
S204
引落し額入力
要求あり
NO
YES
S205
不適正の返信
あり
NO
YES
S207
不適正である旨
の表示
RET
S206
引落し額の入力
指示表示
S208
NO
入力あり
YES
S209
入力された引落し
額Gを送信
S210
NO
G受信
YES
S211
引落し額GをVP用
IC端末へ伝送
RET

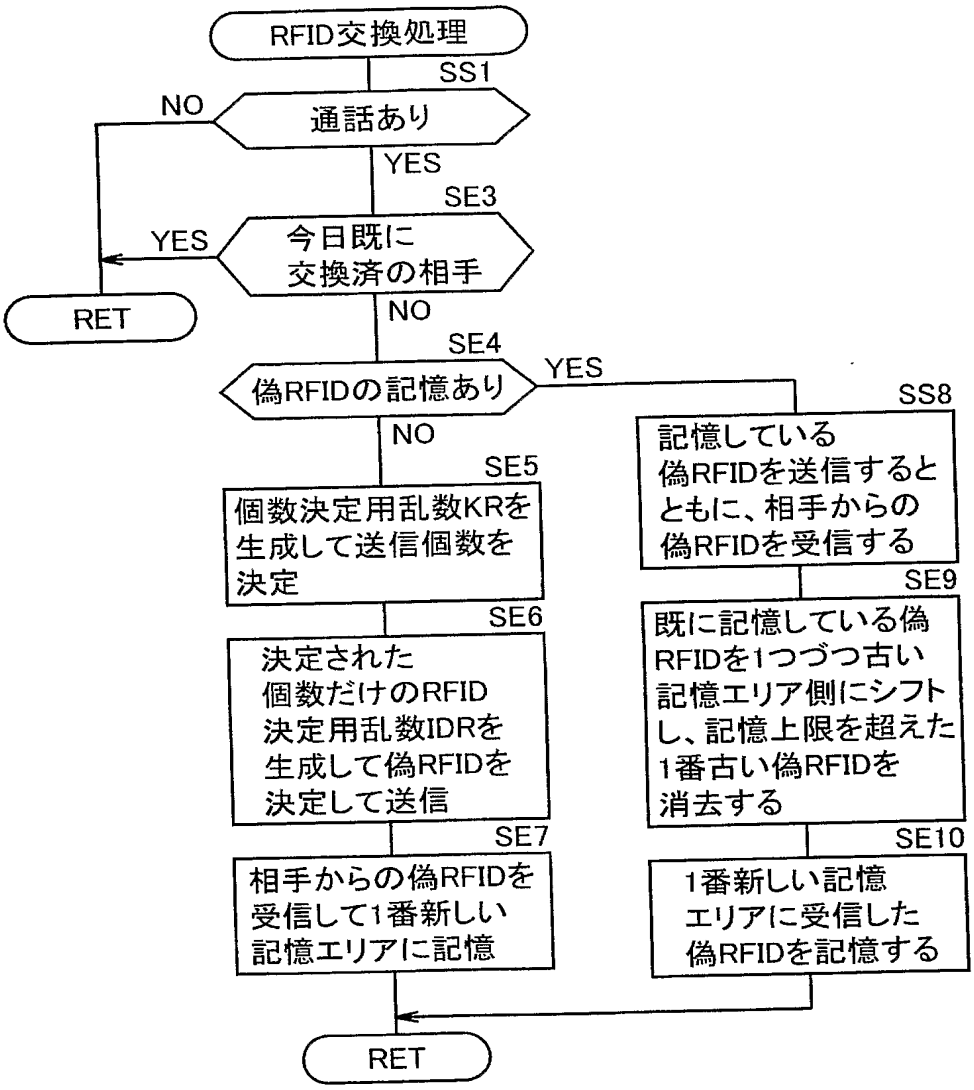
【図５４】


(a)
本人証明処理
S215
NO
乱数R受信
YES
S216
RをIC端末へ伝送
S217
NO
レスポンスデータI受信
YES
S218
Iを送信する
RET
(b)
10
S220
デビットカード使用操作あり
NO
11
YES
S235
デビットカード使用要求を決済サーバへ送信
S221
正当機関チェック処理
S222
NO
R = DKP(L)
YES
S224
暗証番号とカード情報の入力要求あり
NO
S223
正当機関でない旨の警告表示
RET
YES
S225
暗証番号の入力指示を表示
S226
NO
入力あり
YES
S227
VP用ICカードからカード情報を呼出し暗証番号とともに送信
S228
YES
不適正の返信あり
S229
不適正の表示
RET
NO
S230
使用金額の入力指示表示
S231
NO
入力あり
YES
S232
使用金額G送信
S233
NO
G受信
YES
S234
決済完了表示
RET

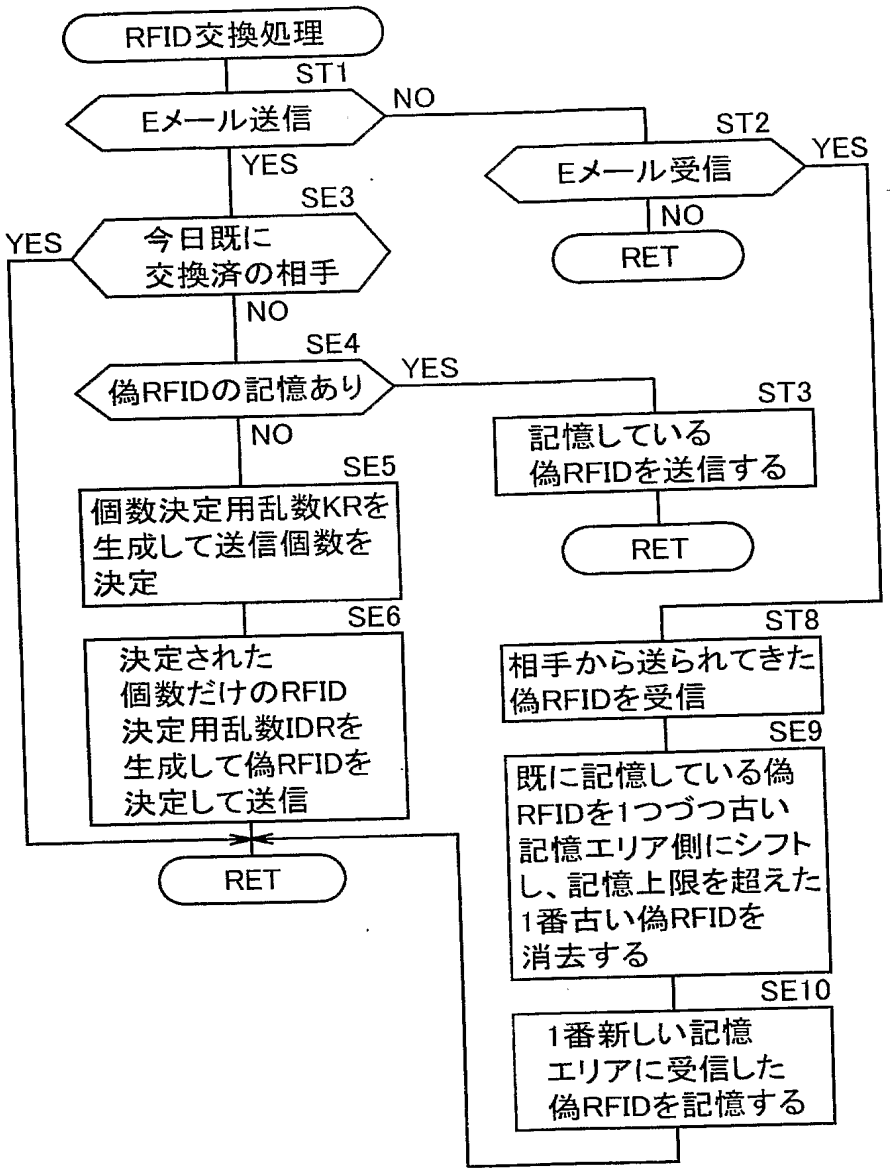
【図５５】


11
S238
クレジットカード使用操作あり
NO
YES
S249
リロード金額の使用操作あり
NO
YES
RET
クレジットカードによる決済要求を加盟店へ送信する
S237
使用金額入力指示
S250
正当機関チェック処理
S239
S251
NO
入力あり
YES
S240
NO
R = DKP(L)
YES
使用金額Gの引落し要求をVP用IC端末へ伝送
S252
S241
正当な販売店でない旨の警告表示
オーダー情報OIと支払指示PI作成
S242
S252a
NO
引落し完了の返信あり
YES
RET
OIとPIのメッセージダイジェストを連結した2重ダイジェストMDを算出
S243
Gの支払処理
S252b
RET
MDとクレジットカードを使用するVP氏名とをVP用IC端末へ伝送して署名指示を出すとともに、VP用電子証明書の出力を要求
S244
S245
NO
署名返信あり
YES
S605
XMLストアへの電子証明書取寄せ指示あり
NO
YES
XMLストアへアクセスして電子証明書を取寄せる
S606
OIとPIと署名としてのD(KS)(MD)とVP用電子証明書とを送信
S246
S247
NO
回答メッセージ受信
YES
取引完了表示
S248
RET

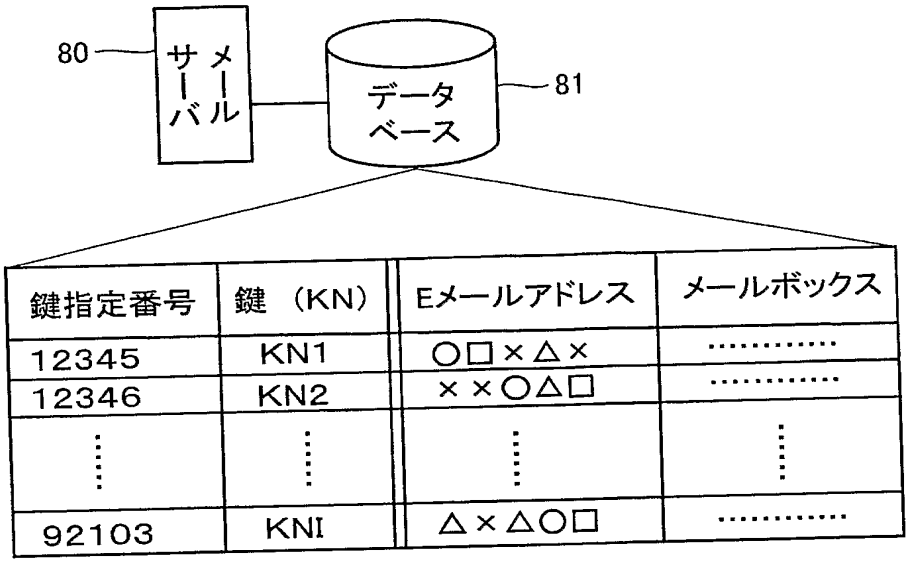
【図５６】


RFID交換処理
SS1
通話あり
NO
YES
SE3
今日既に
交換済の相手
YES
RET
NO
SE4
偽RFIDの記憶あり
YES
NO
SS8
記憶している
偽RFIDを送信すると
ともに、相手からの
偽RFIDを受信する
SE5
個数決定用乱数KRを
生成して送信個数を
決定
SE9
既に記憶している偽
RFIDを1つづつ古い
記憶エリア側にシフト
し、記憶上限を超えた
1番古い偽RFIDを
消去する
SE6
決定された
個数だけのRFID
決定用乱数IDRを
生成して偽RFIDを
決定して送信
SE10
1番新しい記憶
エリアに受信した
偽RFIDを記憶する
SE7
相手からの偽RFIDを
受信して1番新しい
記憶エリアに記憶
RET

【図５７】

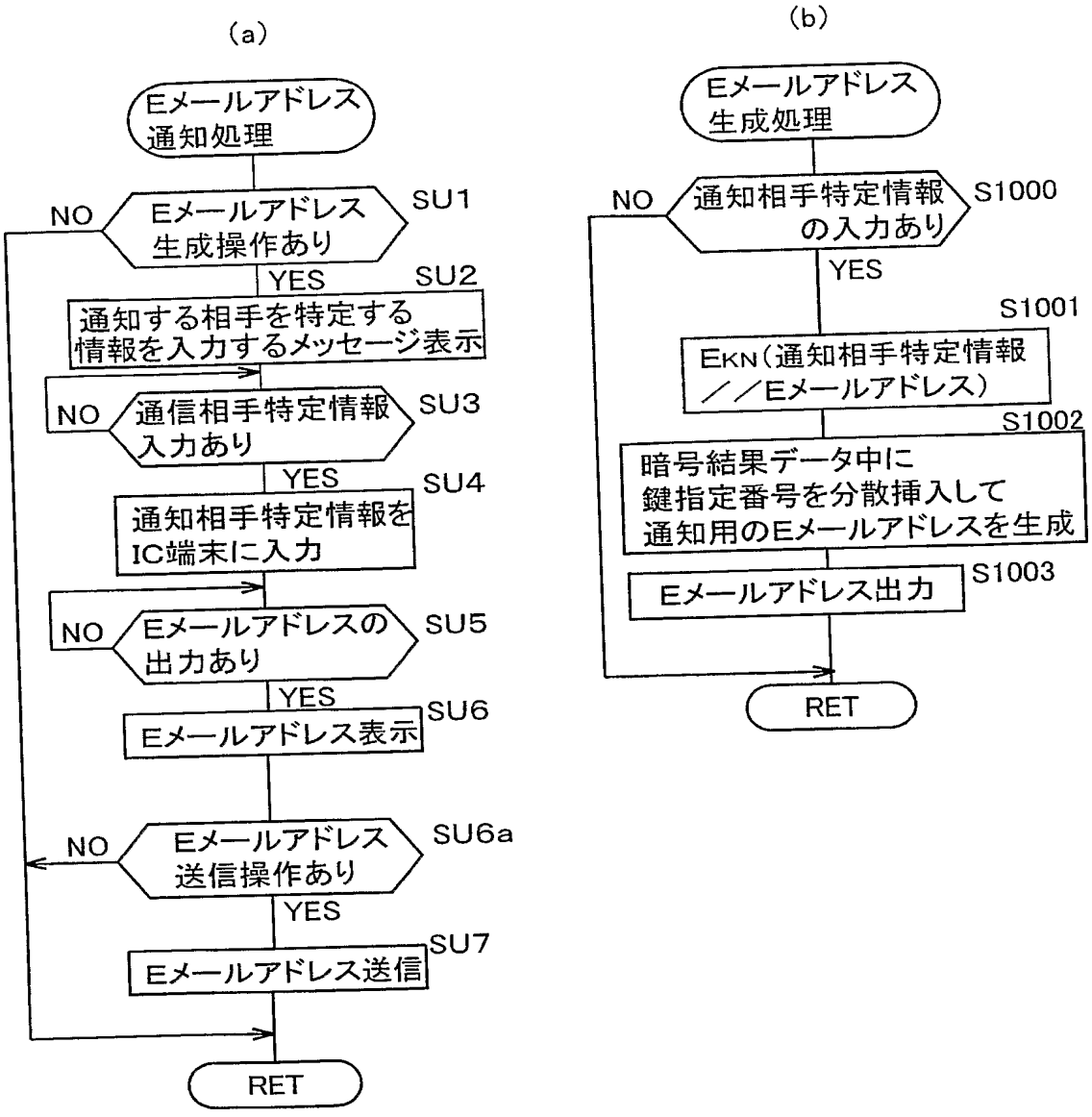

RFID交換処理
ST1
Eメール送信
NO
YES
ST2
Eメール受信
YES
NO
RET
SE3
今日既に
交換済の相手
YES
NO
SE4
偽RFIDの記憶あり
YES
NO
ST3
記憶している
偽RFIDを送信する
RET
SE5
個数決定用乱数KRを
生成して送信個数を
決定
SE6
決定された
個数だけのRFID
決定用乱数IDRを
生成して偽RFIDを
決定して送信
RET
ST8
相手から送られてきた
偽RFIDを受信
SE9
既に記憶している偽
RFIDを1つづつ古い
記憶エリア側にシフト
し、記憶上限を超えた
1番古い偽RFIDを
消去する
SE10
1番新しい記憶
エリアに受信した
偽RFIDを記憶する

【図５８】

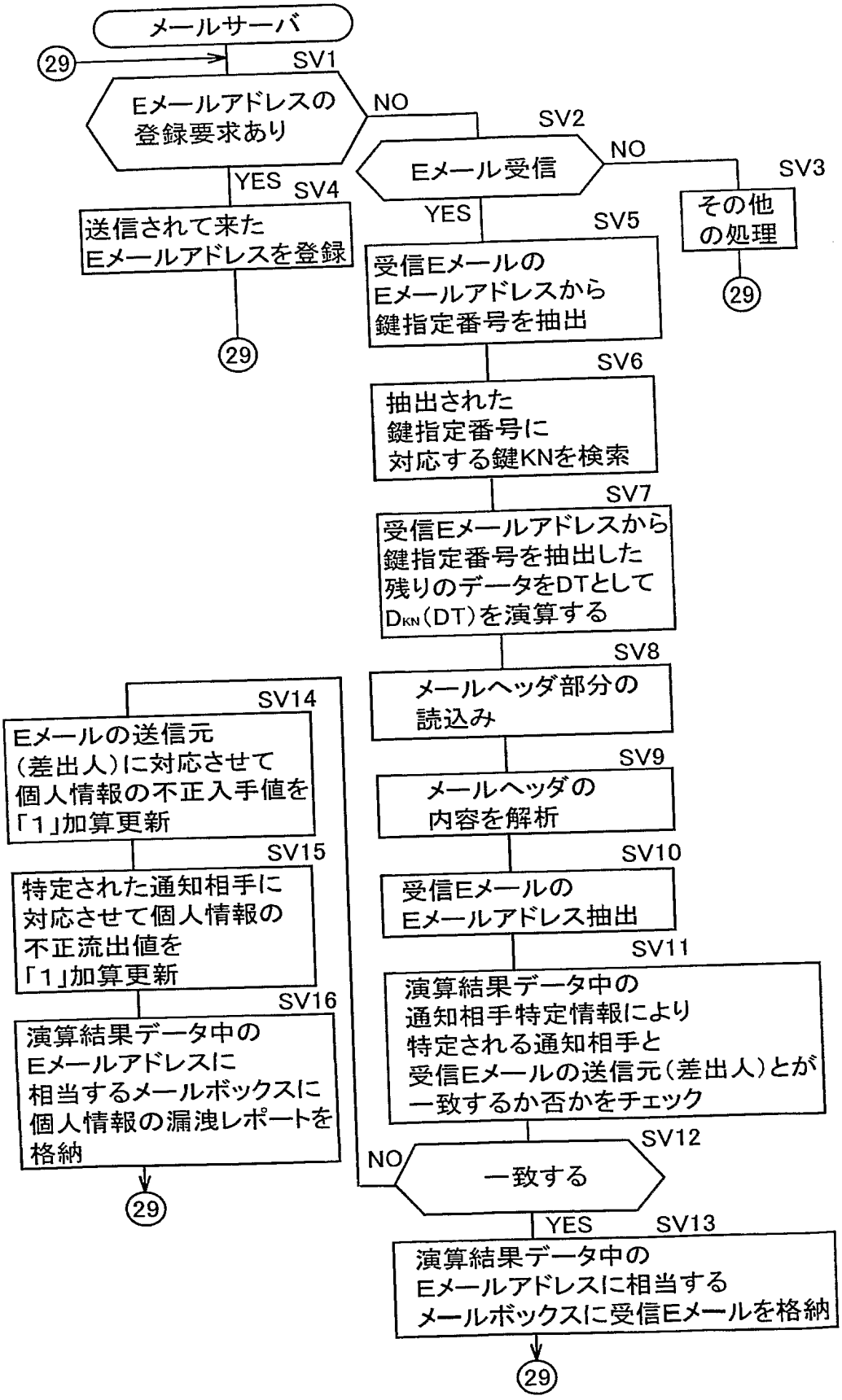


鍵指定番号	鍵　（KN）	Eメールアドレス	メールボックス
12345	KN1	○□×△×	……
12346	KN2	××○△□	……
⋮	⋮	⋮	⋮
92103	KNI	△×△○□	……

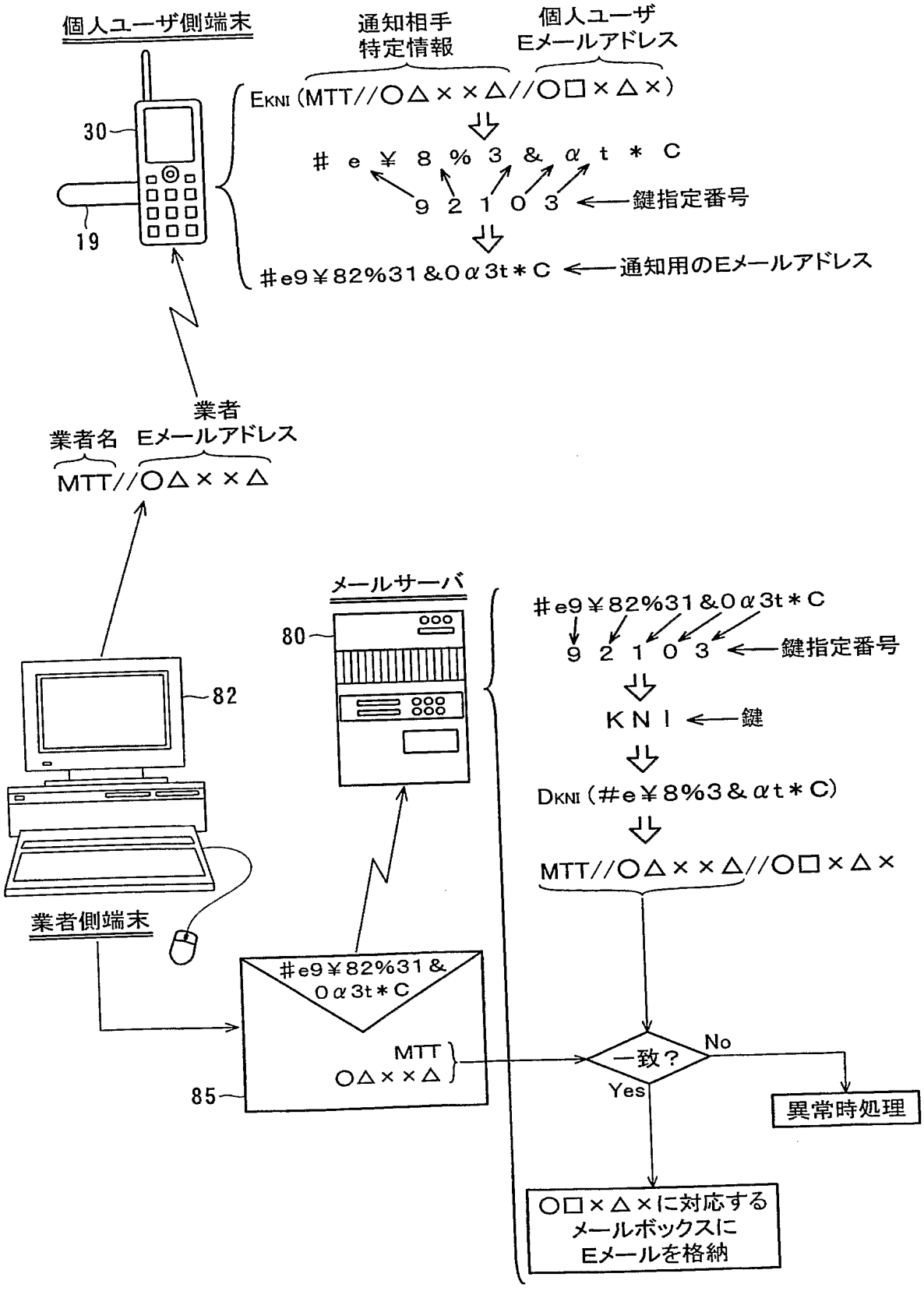
【図５９】


(a)
Eメールアドレス
通知処理
NO
Eメールアドレス
生成操作あり
SU1
YES
SU2
通知する相手を特定する
情報を入力するメッセージ表示
NO
通信相手特定情報
入力あり
SU3
YES
SU4
通知相手特定情報を
IC端末に入力
NO
Eメールアドレスの
出力あり
SU5
YES
SU6
Eメールアドレス表示
NO
Eメールアドレス
送信操作あり
SU6a
YES
SU7
Eメールアドレス送信
RET
(b)
Eメールアドレス
生成処理
NO
通知相手特定情報
の入力あり
S1000
YES
S1001
EKN(通知相手特定情報
／／Eメールアドレス)
S1002
暗号結果データ中に
鍵指定番号を分散挿入して
通知用のEメールアドレスを生成
Eメールアドレス出力
S1003
RET

【図６０】


メールサーバ
29
SV1
Eメールアドレスの登録要求あり
NO
SV2
Eメール受信
NO
SV3
その他の処理
29
YES
SV4
送信されて来たEメールアドレスを登録
29
YES
SV5
受信Eメールの Eメールアドレスから 鍵指定番号を抽出
SV6
抽出された 鍵指定番号に 対応する鍵KNを検索
SV7
受信Eメールアドレスから 鍵指定番号を抽出した 残りのデータをDTとして DKN(DT)を演算する
SV8
メールヘッダ部分の読込み
SV9
メールヘッダの内容を解析
SV10
受信Eメールの Eメールアドレス抽出
SV11
演算結果データ中の 通知相手特定情報により 特定される通知相手と 受信Eメールの送信元(差出人)とが 一致するか否かをチェック
SV12
NO
一致する
YES
SV13
演算結果データ中の Eメールアドレスに相当する メールボックスに受信Eメールを格納
29
SV14
Eメールの送信元 (差出人)に対応させて 個人情報の不正入手値を 「1」加算更新
SV15
特定された通知相手に 対応させて個人情報の 不正流出値を 「1」加算更新
SV16
演算結果データ中の Eメールアドレスに 相当するメールボックスに 個人情報の漏洩レポートを 格納
29

【図６１】


個人ユーザ側端末
通知相手
特定情報
個人ユーザ
Eメールアドレス
EKNI（MTT//○△××△//○□×△×）
30
19
＃ｅ￥８％３＆αｔ＊Ｃ
９２１０３
鍵指定番号
＃e9￥82%31&0α3t＊C
通知用のEメールアドレス
業者
業者名
Eメールアドレス
MTT//○△××△
メールサーバ
80
82
＃e9￥82%31&0α3t＊C
９２１０３
鍵指定番号
ＫＮＩ
鍵
DKNI（＃ｅ￥８%３＆αｔ＊C）
MTT//○△××△//○□×△×
業者側端末
＃e9￥82%31&
0α3t＊C
MTT
○△××△
85
一致？
No
Yes
異常時処理
○□×△×に対応する
メールボックスに
Eメールを格納

【書類名】要約書
【課題】
読取られた固有の識別子に基づいて行われるプライバシーの侵害を防止する。
【解決手段】
個人ユーザが業者ＭＴＴにＥメールアドレスを通知するにおいて、通知相手の業社名ＭＴＴおよびＥメールアドレスからなる通知相手特定情報と自己のＥメールアドレスとを暗号化（E_{KNI}（ＭＴＴ//○△××△//○□×△×））して通知用Ｅメールアドレスを生成して通知する。ＭＴＴからＲＦＩＤ発信要求があればＭＴＴ専用のＲＦＩＤを発信する一方、ＭＴＴ以外（たとえばＭＥＣ）からＲＦＩＤ発信要求があった場合も操作に応じてＭＴＴ専用のＲＦＩＤを発信する。そのＭＴＴ専用ＲＦＩＤとリンクした個人情報がＭＴＴから漏洩した後、ＭＴＴ専用ＲＦＩＤを受信したＭＥＣが漏洩個人情報を検索して入手し、その個人情報中の通知用Ｅメールアドレス宛にＥメール８５を送信した場合に、通知用Ｅメールアドレスを復号して得た通知相手特定情報ＭＴＴ//○△××△とＥメールの送信元ＭＥＣとが一致せず、個人情報の漏洩元と入手先とを特定できる。
【選択図】　図６１

特願２００４－１８２１８０

出　願　人　履　歴　情　報

識別番号　［５０２１７８１２６］

１．変更年月日　２００２年　４月　９日
［変更理由］　新規登録
住　所　岡山県倉敷市羽島２２１番地の４
氏　名　石井　美恵子